

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-217894

(P 2 0 0 2 - 2 1 7 8 9 4 A)

(43) 公開日 平成14年8月2日(2002.8.2)

(51) Int. Cl. <sup>7</sup>	識別記号	F I	ターマコード (参考)
H04L 9/08		G06F 13/00	520 B 5C052
G06F 13/00	520	17/60	302 E 5C053
17/60	302		332 5C064
	332		ZEC 5J104
	ZEC	H04N 5/76	Z
審査請求 未請求 請求項の数17 O L (全43頁) 最終頁に続く			

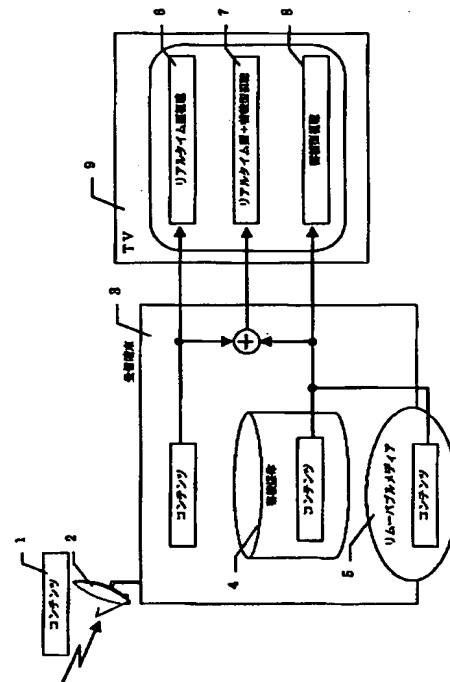
(21) 出願番号	特願2001-295722(P 2001-295722)	(71) 出願人	000005108 株式会社日立製作所 東京都千代田区神田駿河台四丁目6番地
(22) 出願日	平成13年9月27日(2001.9.27)	(72) 発明者	原田 宏美 東京都千代田区神田駿河台四丁目6番地 株式会社日立製作所放送・通信システム推進事業部内
(31) 優先権主張番号	特願2000-300566(P 2000-300566)	(72) 発明者	小西 薫 東京都千代田区神田駿河台四丁目6番地 株式会社日立製作所放送・通信システム推進事業部内
(32) 優先日	平成12年9月28日(2000.9.28)	(74) 代理人	100107010 弁理士 橋爪 健
(33) 優先権主張国	日本 (J P)		最終頁に続く

(54) 【発明の名称】 データ配信サービス方法

(57) 【要約】

【課題】 コンテンツに関する詳細な情報を用いてのコンテンツ制御サービスを行う。

【解決手段】 放送サイドで視聴者へのコンテンツ提示方法、利用条件、暗号化状態でのコンテンツ蓄積、端末に対する限定受信、個人に対する限定受信等を定義し、定義した内容をコンテンツと共に受信側に配信し、これらの定義に基づき視聴者の視聴制御、蓄積制御、コピー制御、暗号/復号制御等を行うことで著作権等のコンテンツの権利保護が可能なサービスを提供する。そのために、総合データ配信システムは、コンテンツ毎にコンテンツ関連情報であるメタデータを添付する。このメタデータには、コンテンツの名称、内容、コンテンツ内の構成等の一般的な情報や、蓄積再生処理に関する制御情報、課金処理に関する制御情報、コンテンツの復号鍵等のコンテンツ暗号方式に関する情報等の著作権保護に関する情報が記述される。



## 【特許請求の範囲】

【請求項1】衛星、地上回線等の通信回線もしくはリム  
ーバブルメディア等のメディア媒体を用いてコンテンツ  
の配信を行うデータ配信サービス方法において、

送信側装置は、

コンテンツの生成後にコンテンツの暗号化を行い、

暗号化されたコンテンツをブロック分けし、

配信ストリームのペイロード部分にブロック分けした暗  
号化コンテンツの各エレメントを格納して、配信データ  
形式に組み立て、コンテンツを配信し、

コンテンツの提示方法、利用条件、コンテンツの暗号鍵  
を含むコンテンツの関連情報を格納したメタデータを生  
成して配信し、

受信端末は、

コンテンツを組み立てる場合にペイロード部分を復号せ  
ずに組み立て、暗号化されたままの状態でのコンテンツ  
及びメタデータを蓄積し、

受信側でコンテンツの利用に関する判断をすることによ  
りコンテンツに対する課金制御、権利保護を行うように  
したデータ配信サービス方法。

【請求項2】請求項1のデータ配信サービス方法におい  
て、

コンテンツの暗号化はコンテンツを構成する各エレメン  
トのデータ全体に暗号化を行い、

メタデータについては予め定められた必要部分にのみ暗  
号化を行うことを特徴とするデータ配信サービス方法。

【請求項3】衛星、地上回線等の通信回線もしくはリム  
ーバブルメディア等のメディア媒体を用いてコンテンツ  
の配信を行うデータ配信サービス方法において、

受信端末は、ユーザーが有料事業者に対し契約した端末  
ID、個人ID、契約したいチャンネル又は番組又はコンテ  
ンツを含む契約要求を送出側装置に通知するステップ  
と、

送出側装置は、通知された契約要求より事前契約用メタ  
データを生成し、端末ID、個人IDを非暗号化とし、有料  
事業者ID、事業者毎に固有の事業者鍵Kw、契約コードを  
含む契約情報を受信端末毎に固有の端末鍵Kmcで暗号化  
を行い、受信端末に配信するステップと、

受信端末は、事前契約用メタデータの非暗号化部分に格  
納されている端末ID、個人IDにより、端末を使用するユ  
ーザー宛の情報か否かを判断し、使用ユーザー宛と判断  
された場合は、受信端末内に予め格納されている端末鍵  
Kmcにより事前契約用メタデータを復号し、事業者鍵Kw  
を含む契約情報を入手するステップと、

受信端末は、入手した契約情報に基づき、契約事業者の  
放送するコンテンツの要求を行うステップと、

送出側装置は、暗号化コンテンツの配信と同期させ、有  
料事業者IDを非暗号化として含み、コンテンツを視聴す  
る際に必要となるコンテンツの暗号鍵Kkを含む必要部分  
が事業者鍵Kwで暗号化された鍵配信用メタデータと、コ

ンテンツ配信装置位置を含むコンテンツに対する利用制  
限情報を含む必要部分をコンテンツ鍵Kkで暗号化された  
蓄積/再生用メタデータとを配信するステップと、

受信端末は、暗号化コンテンツと同期させて配信される  
鍵配信用メタデータを受信し、非暗号化部分に格納され  
ている有料事業者IDにより契約事業者による放送かを判  
断し、契約する事業者の放送するコンテンツに対する鍵  
配信用メタデータであると判断した場合、事前契約用メ  
タデータにより配信された事業者鍵Kwにより暗号化部分  
を復号し、復号された対象契約コードと事前契約用メタ  
データにより配信された契約コードとによりユーザーの  
契約形態内で利用可能なコンテンツかを判断し、利用可  
能であればコンテンツ鍵Kkを受信端末に格納し、同時に  
受信した蓄積/再生用メタデータの暗号化部分をコンテ  
ンツ鍵Kkにより復号し、コンテンツに対する利用制限情  
報を確認し、ユーザーの利用が可能であれば、蓄積/再  
生用メタデータに格納されている暗号化コンテンツの配  
信場所の情報により暗号化コンテンツを受信するステッ  
プとを含むデータ配信サービス方法。

20 【請求項4】請求項1又は3に記載のデータ配信サービ  
ス方法において、

ユーザーに対して様々なコンテンツ単位、チャンネル単  
位、番組単位又はパソコンにおけるファイル単位などの  
エレメント単位のサービスを提供するために、送出側装  
置は、コンテンツの物理量を示す単位を指定し、指定し  
た物理量をメタデータに含ませて配信することにより、  
受信端末が指定されたコンテンツ単位でサービスを提供  
可能とすることを特徴としたデータ配信サービス方法。

30 【請求項5】請求項1又は3に記載のデータ配信サービ  
ス方法において、

メタデータは、コンテンツのタイトル又は内容、送出側  
で定義した視聴者へのコンテンツ提示方法、利用条件を  
含む情報を含み、

送出側装置は、メタデータ自体もデータの改ざん防止、

秘匿性保持のため必要部分を暗号化したのち配信し、

受信端末は、暗号化されたままの状態でメタデータを蓄  
積し、利用時に暗号鍵により受信端末を制御して権利保  
護を行うことを特徴とするデータ配信サービス方法。

40 【請求項6】請求項1又は3のデータ配信サービス方法  
において、

事前契約用メタデータは、有料放送事業者の事業者鍵K  
w、契約形態に間する契約コード内容を含み、端末購入  
時、契約更新時又は事業者鍵Kwの更新時に配信されるメ  
タデータであって、

EPG用メタデータは、配信予定コンテンツの確認又は予  
約を行うためのメタデータであり、

蓄積/再生用メタデータは、コンテンツの受信、蓄積、  
再生に必要な情報を含むメタデータであり、

50 鍵配信用メタデータは、コンテンツの暗号鍵に関する情  
報を配信するメタデータであり、

メタデータリストは、配信ストリーム中の各メタデータの配信位置を取得するためのメタデータであり、システム鍵更新用メタデータは、全受信端末共通のシステム鍵Ksyを更新するためのメタデータであり、送信側装置は、受信端末側での使用目的、送出側での配信タイミング、記述内容によりメタデータを、事前契約用メタデータ、EPG用メタデータ、蓄積/再生用メタデータ、鍵配信用メタデータ、システム鍵更新用メタデータ、メタデータリストに区分けして、配信することの特徴とするデータ配信サービス方法。

【請求項7】請求項6に記載のデータ配信サービス方法において、

ユーザーに対して個別に配信される事前契約用メタデータは、ユーザー個々の契約情報が格納され、全ユーザーに対して共通的に配信される各コンテンツに対する鍵配信用メタデータ、蓄積/再生用メタデータは、必要となる契約情報、利用条件等が格納され、事前契約用メタデータにより配信されたユーザー個々の契約情報と他のメタデータに含まれる契約情報とを照合してユーザーのコンテンツ利用を判断することで、ユーザー個々に対しコンテンツ単位の限定受信を行うようにしたことを特徴とするシステム。

【請求項8】請求項6に記載のデータ配信サービス方法において、

事前契約用メタデータは、ユーザー毎の契約情報や事業者毎の事業者鍵Kwを含む権利保護が必要な情報が格納され、送出側装置は、この情報を各ユーザーの所有する端末毎の端末鍵Kmc又は個人鍵Kmにより暗号化することにより情報の秘匿を守り情報を配信することの特徴とするデータ配信サービス方法。

【請求項9】請求項6に記載のデータ配信サービス方法において、

EPG用メタデータは、配信予定コンテンツの確認又は予約を行うもので、利用制限情報を含む権利保護が必要な情報が格納され、

送出側装置は、この情報を全受信端末で共通な鍵Ksyにより暗号化することによりユーザーの区別無く全ユーザーに対してメタデータ内の必要な情報の秘匿性を保持したまま配信することの特徴とするデータ配信サービス方法。

【請求項10】請求項6に記載のデータ配信サービス方法において、

コンテンツに対する暗号鍵を含む情報を格納した鍵配信用メタデータ、コンテンツのコピーコントロール情報を含む情報を格納した蓄積再生用メタデータについて、送出側装置は、鍵配信用メタデータを事業者鍵Kw、蓄積再生用メタデータをコンテンツ毎のコンテンツ鍵Kkにより暗号化し配信することで、事業者と契約を行い事前契約用メタデータにより事業者鍵を受け取ったユーザーのみコンテンツ鍵Kkを取得可能とすることでコンテンツの権

利保護を実現することを特徴とするデータ配信サービス方法。

【請求項11】請求項6に記載のデータ配信サービス方法において、

鍵配信用メタデータは、コンテンツの暗号鍵に関する情報を配信するものであり、

送出側装置は、コンテンツが有料放送の場合は、その情報を事業者毎に固有の事業者鍵Kwにより暗号化し、契約者以外のユーザーも視聴可能な無料コンテンツに対するメタデータの場合は、全受信端末に共通なシステム鍵Ksyにより暗号化すること。

【請求項12】請求項6に記載のデータ配信サービス方法において、

システム鍵更新用メタデータは、システム内の全受信端末で共通なシステム鍵を含むシステム全体で共通的な情報を更新するための情報が格納されたメタデータであり、

送出側装置は、新しいシステム鍵Ksy3を含む保護が必要な部分を予め全受信端末内で共通に用意された予備用のシステム鍵Ksy2を用いて暗号化することでユーザーの区別なくメタデータ内の必要な部分の秘匿性を保持したまま配信可能とすることを特徴とするデータ配信サービス方法。

【請求項13】請求項6に記載のデータ配信サービス方法において、

メタデータリストは、配信中の各メタデータリストの伝送路上の配信位置を格納し、受信端末は、メタデータリストを用いてメタデータの取得を行うことを特徴とするデータ配信サービス方法。

【請求項14】請求項6に記載のデータ配信サービス方法において、

メタデータリストにEPG用メタデータ、蓄積再生用メタデータ等の更新を識別するための情報を格納することにより更新されたメタデータのみ受信を行うことを可能とすることを特徴とするに記載のデータ配信サービス方法。

【請求項15】請求項1又は3のデータ配信サービス方法において、

暗号化されたメタデータを、暗号化を行わないメタデータに再度埋め込み配信する場合と、別ファイルとして配信する場合とのいずれかにより配信すること。

【請求項16】請求項1又は3のデータ配信サービス方法において、

送出側装置は、受信端末を購入したユーザーが端末ID、個人ID、契約したい事業者、コンテンツを利用するためのポイント数を含む情報を元に顧客情報を生成管理し、許諾するポイント数の情報を事前契約用メタデータに格納し、契約ユーザーの受信端末に配信し、

送出側装置は、コンテンツを配信する際に同期させ、配信させる蓄積/再生用メタデータにコンテンツを利用す

る際に必要となるポイント数の情報を格納して配信し、受信端末は、コンテンツを利用する際に、事前契約用メタデータにより配信されたポイント数より蓄積/再生用メタデータに格納されている必要ポイント数を減算し、コンテンツの再生を行うことで、事前契約用メタデータで配信されたポイント数の範囲でのコンテンツを視聴することを特徴とするデータ配信サービス方法。

【請求項17】請求項1又は3データ配信サービス方法において、

送出側装置は、受信端末を購入したユーザーが端末ID、個人ID、契約したい事業者、コンテンツを利用するためのポイント数を含む情報を元に顧客情報を生成管理し、オンラインペーパービュー許諾として、課金情報送信時の送信先の情報を事前契約用メタデータに格納し、契約ユーザーの受信端末に配信し、

送出側装置は、コンテンツを配信する際に同期させ、配信させる蓄積/再生用メタデータにコンテンツを利用する際の課金情報を生成する元となる情報を格納し配信する受信端末は、コンテンツを利用する際に、蓄積/再生用メタデータに格納された課金情報を生成するための元となる情報に対し利用ユーザーのIDを含む情報を加え、事前契約用メタデータにより指定された送信先に対し地上回線を利用して送信することを特徴とするデータ配信サービス方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンテンツ提供側においてコンテンツを提供し、利用側においてコンテンツを受け取り、利用するためのデータ配信サービス方法に係り、特に、コンテンツを保護する仕組みを備え且つコンテンツにコンテンツ関連情報であるメタデータを付加して配信する仕組みを備えたデータ配信サービス方法に関する。

【0002】

【従来の技術】従来、衛星波や地上波を用いた放送または通信は、リアルタイム放送が一般的であり、一部、蓄積型の通信が存在していた。蓄積型の放送や通信は、配信された番組や情報をユーザー自身の蓄積動作によって、大容量の蓄積媒体に蓄積することが可能である。よって、ユーザーが望む時にいつでも、番組を視聴することができる。

【0003】リアルタイム放送のコンテンツの保護方法として、コンテンツに暗号をかける方式が一般的である。暗号をかけることにより、不正な視聴や改ざんなどが困難となる。コンテンツ暗号方式として、BSデジタル放送の限定受信方式であるCAS(Conditional Access System)がある。CASはコンテンツを第1の暗号方式で暗号化し、その暗号化コンテンツを復号するための第1の復号鍵を第2の暗号方式で暗号化する。そして、暗号化コンテンツと第1の鍵をユーザーに対して配信する。その

コンテンツを受信可能なユーザーは、予め第2の暗号方式の復号鍵である第2の復号鍵を保持している。よって、第2の復号鍵を保持しているユーザーのみ第1の復号鍵を受信することができ、第1の復号鍵を受信できたユーザーのみがコンテンツを受信することが可能である。このように、CASを用いることで、限定されたユーザーのみコンテンツを入手し視聴することが可能となり、視聴可能なユーザーをコントロールすることが可能である。また、BSデジタル放送では、コンテンツに関する情報としてSI(サービス情報)が定義されている。

【0004】

【発明が解決しようとする課題】上述のような従来技術のCASは、リアルタイム放送で用いられている限定受信方式である。この方式はコンテンツの受信と同時にコンテンツの復号処理を行う。その際、ユーザーに対する受信コントロールは可能であるが、コンテンツを復号してしまうため再生コントロールができない。また、蓄積時にコンテンツが平文状態となってしまうのでコンテンツの保護ができない。

【0005】また、現状の衛星デジタル放送の規格においては、コンテンツに関する情報を定義するための手段として、SIのみしか存在しない。このSIはコンテンツの関連情報ではあるがEPG(電子番組ガイド)用の情報なので、詳細に記述されているわけではない。様々なコンテンツに関する詳細な情報を定義する手段は放送規格においてはなため、コンテンツ毎の制御に基づいた木目細かいサービスを行うことができない。これにより、コンテンツに関する詳細な情報を用いてのコンテンツ制御サービスは行うことができない。また、既存型の放送はコンテンツをリアルタイムで視聴することを念頭においたサービスであるため、コンテンツの蓄積制御、コピー制御を行うための情報が乏しく蓄積型放送に使用するには不十分である。

【0006】本発明は、以上の点に鑑み、蓄積型放送かつ、コンテンツの保護が可能となる制御情報を付加するデータ配信サービス方法を提供することを目的とする。

【0007】

【課題を解決するための手段】本発明の総合データ配信システムは、暗号化した状態のコンテンツを受信し、その後蓄積媒体に蓄積し、コンテンツの再生時に初めて復号する暗号方式を提供する。また、コンテンツ毎にコンテンツ関連情報であるメタデータを添付する。このメタデータには、例えば、コンテンツの名称、内容、コンテンツ内の構成等の一般的な情報や、蓄積再生処理に関する制御情報、課金処理に関する制御情報、コンテンツの復号鍵等のコンテンツ暗号方式に関する情報等の著作権保護に関する情報が記述される。これらの情報に基づき視聴者の視聴制御、蓄積制御、コピー制御、暗号/復号制御等を行う。これよりコンテンツの権利保護、ユーザーの権利保護等が可能となる。

【0008】本発明の第1の解決手段によると、衛星、地上回線等の通信回線もしくはリムーバブルメディア等のメディア媒体を用いてコンテンツの配信を行うデータ配信サービス方法において、送信側装置は、コンテンツの生成後にコンテンツの暗号化を行い、暗号化されたコンテンツをブロック分けし、配信ストリームのペイロード部分にブロック分けした暗号化コンテンツの各エレメントを格納して、配信データ形式に組み立て、コンテンツを配信し、コンテンツの提示方法、利用条件、コンテンツの暗号鍵を含むコンテンツの関連情報を格納したメタデータを生成して配信し、受信端末は、コンテンツを組み立てる場合にペイロード部分を復号せずに組み立て、暗号化されたままの状態でのコンテンツ及びメタデータを蓄積し、受信側でコンテンツの利用に関する判断をすることによりコンテンツに対する課金制御、権利保護を行うようにしたデータ配信サービス方法が提供される。

【0009】本発明の第2の解決手段によると、衛星、地上回線等の通信回線もしくはリムーバブルメディア等のメディア媒体を用いてコンテンツの配信を行うデータ配信サービス方法において、受信端末は、ユーザーが有料事業者に対し契約した端末ID、個人ID、契約したいチャンネル又は番組又はコンテンツを含む契約要求を送出側装置に通知するステップと、送出側装置は、通知された契約要求より事前契約用メタデータを生成し、端末ID、個人IDを非暗号化とし、有料事業者ID、事業者毎に固有の事業者鍵Kw、契約コードを含む契約情報を受信端末毎に固有の端末鍵Kmcで暗号化を行い、受信端末に配信するステップと、受信端末は、事前契約用メタデータの非暗号化部分に格納されている端末ID、個人IDにより、端末を使用するユーザー宛の情報が否かを判断し、使用ユーザー宛と判断された場合は、受信端末内に予め格納されている端末鍵Kmcにより事前契約用メタデータを復号し、事業者鍵Kwを含む契約情報を入手するステップと、受信端末は、入手した契約情報に基づき、契約事業者の放送するコンテンツの要求を行うステップと、送出側装置は、暗号化コンテンツの配信と同期させ、有料事業者IDを非暗号化として含み、コンテンツを視聴する際に必要となるコンテンツの暗号鍵Kkを含む必要部分が事業者鍵Kwで暗号化された鍵配信用メタデータと、コンテンツ配信装置位置を含むコンテンツに対する利用制限情報を含む必要部分をコンテンツ鍵Kkで暗号化された蓄積/再生用メタデータとを配信するステップと、受信端末は、暗号化コンテンツと同期させて配信される鍵配信用メタデータを受信し、非暗号化部分に格納されている有料事業者IDにより契約事業者による放送かを判断し、契約する事業者の放送するコンテンツに対する鍵配信用メタデータであると判断した場合、事前契約用メタデータにより配信された事業者鍵Kwにより暗号化部分を復号し、復号された対象契約コードと事前契約用メタデータ

により配信された契約コードとによりユーザーの契約形態内で利用可能なコンテンツかを判断し、利用可能であればコンテンツ鍵Kkを受信端末に格納し、同時に受信した蓄積/再生用メタデータの暗号化部分をコンテンツ鍵Kkにより復号し、コンテンツに対する利用制限情報を確認し、ユーザーの利用が可能であれば、蓄積/再生用メタデータに格納されている暗号化コンテンツの配信場所の情報により暗号化コンテンツを受信するステップとを含むデータ配信サービス方法が提供される。

#### 【0010】

##### 【発明の実施の形態】 1. 概要

(サービス概要) 本総合データ配信サービスとは、見たいコンテンツを見たい時に見たい場所で見られる情報(データ)配信サービスであり、従来のリアルタイム型(放送しているものを視聴する)デジタル放送とは異なり、リアルタイム型に限らず蓄積型の情報配信をも行うサービスである。これにより視聴者が、何時でも好きなときに蓄積されたコンテンツの中から好みのコンテンツを選んで視聴することが可能なニアビデオオンデマンド(NVOD: Near Video On Demand)的なサービスが提供される。また、リムーバブルメディア、本サービスを受信する受信端末に接続される外部機器に直接コンテンツを蓄積させるもしくは、コピーすることによりユーザーの好きな場所でのコンテンツ視聴をも提供する。さらに従来のデジタル放送サービスでは端末単位での契約等の狭い範囲でのコンテンツ利用契約形態のみであったが、本サービスではユーザー個人単位での契約等も可能な広範囲のコンテンツ利用契約形態を提供する。

【0011】図1に、総合データ配信サービスの受信側の構成図を示す。本総合データ配信サービスの概要として、蓄積型テレビ放送について図1を用い説明する。受信側では、アンテナ2、受信端末3及びテレビ9を備える。蓄積型テレビ放送とは従来のテレビ放送と同様に放送サイド(放送局)から送られてくるコンテンツ1(番組)をアンテナ2(ケーブルでの配信、パッケージでの配信の場合もある)、受信端末3で受信しテレビ9などのモニタ装置にて配信されてくるその瞬間から視聴を行う、ここではリアルタイム型視聴6と呼ぶ場合に加え、従来のビデオデッキ等と同様に一度配信されてきたコンテンツを蓄積媒体4(ハードディスク等の大容量蓄積媒体)に蓄積後視聴する蓄積型視聴8(DVD-RAM等の可搬性に富んだりリムーバブルメディア5を蓄積媒体として使用することもある)、蓄積されたコンテンツと配信中のリアルタイム視聴型のコンテンツを合わせて視聴するリアルタイム型+蓄積型視聴7などのサービスを可能とする情報配信サービスである。

【0012】(システム概要) 図2に、総合データ配信サービスの全体システム構成図を示す。本総合データ配信サービスを行うシステムとしては、衛星放送、地上波放送など電波によるインフラの他にケーブルテレビ、イ

インターネットなどの通信線を利用したインフラでのサービスが可能であるが、本発明では一例として、図2のような衛星を利用したデジタル衛星放送をインフラとした場合について述べる。

【0013】総合データ配信サービスが提供されるシステムの概要について図2を用いて説明する。本総合データ配信サービスのシステムは送出側100、受信側200、送出側100と受信側200を結ぶ伝送路である衛星を利用した衛星回線10、地上回線11、流通網12、携帯電話網13を備える。ここでいう受信側200とは、必ずしも家庭201に設置される受信端末3のみでなく、自動販売機のような公衆端末202、コンビニエンスストア等の店舗203に設置される端末、移動体である自動車等に搭載される車載端末204、携帯端末205等も想定する。送出側100では、コンテンツ1及び制御情報等を制作、管理し受信側200へ配信する配信センタ、コンテンツの暗号化等に使用する鍵を生成管理する鍵管理センタ、受信側のユーザーの情報を管理する顧客管理センタ、受信側のユーザーからのリクエスト、視聴履歴収集等の地上回線11、携帯電話206を利用した通信を管理する地上回線管理センタ、ユーザー、販売店等に対してDVD等のパッケージメディアによるコンテンツの配信（配達）を行う物流管理センタ等を備える。

【0014】（サービス内容）次に図2のシステムにおいて行われるサービスについて説明する。本総合データ配信サービスにおけるサービスとしては、例えば、第1に前述したように衛星デジタル回線10を主に利用しデジタル情報としての、ビデオ、音楽、電子雑誌、ゲーム等の映像、音声、データによる総合データを家庭に設置される受信端末3に向けて配信する家庭向けサービス300がある。第2に、家庭向けサービス300と同様に自動販売機202、販売店203に対しデータを配信し、家庭内で容量的に蓄積しきれないデータ、蓄積をしていないデータのバックアップ、自動販売機、販売店のみで販売可能なデータ等を扱い、例えば販売店でのみ販売可能な電子雑誌を購入し、家庭の受信端末3で視聴を行う自動販売機/販売店向けサービス301がある。第3に、車載機器204、携帯端末205などの外部機器に対し家庭内の受信端末3、もしくは自動販売機202、販売店203などからコンテンツを携帯し家庭外で視聴を行うことを可能とし、例えば家庭の受信端末に配信された地図データをDVD等のリムーバブルメディア、ICカードを利用することにより車載機器204に持ち出し車の中で利用したり、音楽データをメモリカード等のリムーバブルメディア、ICカードを利用することにより持ち出し携帯端末205により再生等を行う移動体向けサービス302がある。第4に、流通網12を利用し衛星回線10で配信出来ないコンテンツ等をCD-ROM、DVD-ROM等のパッケージメディアにより配信を行い、例えば

ドラマ等のコンテンツを受信端末より予約すると、送出側よりDVD-ROM等で家庭に対しコンテンツを宅配便等で配信するパッケージデリバリーサービス303がある。第5に、携帯電話206等の通信手段を有する外部機器を利用し、送出側を介し家庭内の受信端末をコントロールすることにより例えば、携帯電話206の画面上のEPG（電子番組ガイド）より外出先から家庭の受信端末に対して番組予約等を行う携帯電話向けサービス304がある。さらに、これらに限定されず、通信インフラ整備に伴い、各種多様の幅広いサービスが可能とされる。本実施の形態では、特に家庭向けサービス300について説明するが、他のサービスにも適用可能である。

【0015】（権利保護方式）本総合データ配信サービスとは、直接家庭などにコンテンツを配信し、家庭内等でデジタルデータでの蓄積/コピー/再生を行うことを目的としたサービスであり、これに伴いデータの改ざん、私的利用を超えるコピー、再生等の著作権等の権利に関わる課題が生じるため、コンテンツの著作権、放送事業者、視聴者など各々の権利を保護、管理する必要がある。

【0016】図3に、総合データ配信サービスにおける権利保護方式の説明図を示す。本総合データ配信サービスにおける権利保護方式について図3を用いて説明する。総合データ配信サービスにおける権利保護方式とは、送出側でコンテンツに対し定義した視聴者へのコンテンツの提示方法、利用条件、コンテンツの暗号鍵等の情報が格納されたメタデータ18を、暗号化したコンテンツ（暗号化コンテンツ）17、その他PSI/SI（Program Specific Information/Service Information）等19と共に配信し、一方、受信端末3側の権利保護機能16（RMP機能）によりメタデータ18を解釈し、コンテンツ17の受信端末3への受信制御、蓄積媒体4、リムーバブルメディア5に対する蓄積制御、コピー制御、暗号/復号制御、TV9などのモニタ装置に対する提示制御、外部機器14に対する認証制御、個人を識別するためのICカード15に対する認証/課金制御等を行う方式である。

【0017】次に送出側より配信されるPSI/SI19、コンテンツ17、メタデータ18について説明する。PSI/SI19とは、従来のデジタル放送と同様に、配信中ストリームより必要なデータを取得するためのデータであり、本総合データ配信サービスでは、メタデータ、暗号化コンテンツ等を取得するために利用する。従来のデジタル放送とのサービスの区別は、PSI中のNIT（Network Information Table）内に格納されるサービスリスト記述子、PMT（Program Map Table）内に格納されるストリーム識別記述子等を利用することにより行うこととする。

【0018】コンテンツ17は、本総合データ配信サービスにおいて、データの改ざん、不正使用を防ぐために

蓄積媒体4、リムーバブルメディア5等に、基本的に暗号化されたままの状態では蓄積される。また総合データ配信サービスにおけるコンテンツ17とは、概念的なものであり一定の物理量を示す単位ではなく、送出側の意図する単位で指定可能であり、指定した物理量をメタデータに記すことにより受信端末はコンテンツを認識可能となる。コンテンツは、例えば、また従来のデジタル放送と同様なチャンネルを指定すれば視聴可能な動画による映像系コンテンツと、主に蓄積したのち視聴することを主眼としたデータ系のコンテンツに分けられる。

【0019】図50に、映像系及びデータ系コンテンツを構成するデータの説明図の一例を示す。本総合データ配信サービスでは、コンテンツを構成するデータ群の各データをエレメントと呼ぶ。よってコンテンツは1つあるいは複数エレメントより構成されるものとなる。メタデータ18とは、本総合データ配信サービスにおいて、例えば、送出側である放送事業者の意図する単位で指定されたコンテンツに対して付与されるコンテンツの内容、構成等の検索等に利用される一般的な情報、著作権者及び関連する権利の保護を送出側で定義した視聴者へのコンテンツ提示方法、利用条件等の情報を含む。メタデータは、これらの情報により端末を制御し、権利保護を可能とする。よって、メタデータにはコンテンツと同様、保護すべき情報が含まれるため、一部を暗号化して配信を行い、蓄積時も暗号化されたままの状態では蓄積される。また、メタデータは配信タイミング、内容により、事前契約用メタデータ、EPG用メタデータ、蓄積/再生用メタデータ、鍵配信用メタデータに分類される。

【0020】事前契約用メタデータは、有料放送事業者毎に固有の鍵である事業者鍵や、契約した事業者の放送する番組の全てが視聴可能か、一部が視聴可能か等を受信端末側で解釈するための契約コード等が格納され、ユーザー個人宛にコンテンツの配信とは非同期に配信される。EPG用メタデータは、受信端末側で配信予定のコンテンツの確認、視聴/蓄積予約を行うために必要となるコンテンツの名称、内容、放送予定日などの情報が格納され、受信端末を使用するユーザーの区別なく対象となるコンテンツの配信以前に全受信端末に向け配信され、主に受信端末のEPG表示、視聴/蓄積予約等を行うためのものである。蓄積/再生用メタデータは、コンテンツの受信、蓄積、コンテンツに対する視聴契約を行うための情報が格納され、受信端末を使用するユーザーの区別なく全受信端末に向け対象となるコンテンツの配信と同期させ配信される。鍵配信用メタデータは、コンテンツの暗号化を行った鍵の情報が格納され、蓄積/再生用メタデータと同様に対象となるコンテンツの配信と同期させ配信される。メタデータリストは、PSI/SIと共に利用することにより蓄積したEPG用メタデータの更新を行うための情報、配信中ストリーム群より必要なデータを取得するための情報が格納され、受信端末を使用するユーザー

一の区別なく全受信端末に向け常時配信される。システム鍵更新用メタデータは、端末内に予め格納されているシステム全体で共通の鍵を更新するための情報が格納され、受信端末を使用するユーザーの区別なく全受信端末に向けコンテンツの配信とは非同期に配信される。

【0021】(暗号化方式) 次に本総合データ配信サービスにおけるコンテンツ、メタデータの暗号化方式について説明する。本総合データ配信サービスにおけるコンテンツ、メタデータの暗号化方式は、暗号化コンテンツ、暗号化メタデータを復号せずに蓄積するため、従来のデジタル放送における配信時に暗号化を行う方式とは異なり、コンテンツ、メタデータの生成時に暗号化を行う方式である。

【0022】図4に、総合データ配信サービスと既存サービスの暗号化方式比較の説明図を示す。本総合データ配信サービスにおける暗号化方式と従来のデジタル放送における暗号化方式の比較を図4を用いて説明する。従来方式では、コンテンツを生成20し、その生成されたコンテンツを暗号化する前に配信時のデータ形態であるTSP21を形成するため、ブロック分けし、TSPのペイロード部分22にブロック分けしたコンテンツの一部23を格納し、その後TSPのペイロード部分を暗号化24するため、受信端末側でコンテンツを組み立てる際に、ペイロード部分を復号する必要がある。一方、本総合データ配信サービスにおける暗号化方式の場合では、送信側で、コンテンツの生成20後にコンテンツの暗号化25を行い、暗号化されたコンテンツをブロック分けし、TSPのペイロード部分22にブロック分けした暗号化コンテンツの一部のブロック26を格納し配信するため、受信端末側でコンテンツを組み立てる場合にペイロード部分を復号せずに組み立て可能となり、送出側で暗号化されたままの状態でのコンテンツ、メタデータの蓄積が可能となる。

【0023】(コンテンツ及びメタデータの暗号化方式) 図5に、コンテンツの暗号化方式の説明図を示す。また、図6に、メタデータの暗号化方式の説明図を示す。次にコンテンツ、メタデータそれぞれの暗号化イメージについてそれぞれ図5、図6を用いて説明する。本総合データ配信サービスにおけるコンテンツの暗号化は、映像系コンテンツ27、データ系コンテンツ28の種別に関係なく各コンテンツを構成する各エレメント毎に暗号化を行う。例えば映像系コンテンツ27がMPEG2-Video(PES)29、MPEG2-AAC(PES)30の2エレメントから構成されている場合、それぞれのエレメント毎にデータ全てに暗号化を行い、暗号化エレメント31、32を生成する。このとき暗号化を行うための暗号鍵33はコンテンツ内では共通な暗号鍵Kk1を使用する。本総合データ配信サービスではコンテンツ毎に割り当てられるこの暗号鍵33をコンテンツ鍵Kk1と呼ぶ。よって、映像系コンテンツ27とは別のコンテンツであるデータ系コ

ンテンツ 28 を構成する各エレメントは別の暗号鍵 34 で暗号化される。このとき暗号鍵 34 には、同様に、コンテンツ内で共通な鍵 Kk2 を使用する。なお、コンテンツ鍵 Kk は、コンテンツ鍵全体の総称である。

【0024】本総合データ配信サービスにおけるメタデータの暗号化は、コンテンツの暗号化とは異なり暗号化が必要なメタデータの全体に暗号化を行うのではなく、図 6 のように暗号化が必要な部分 35 のみ抽出し暗号化を行い、暗号化したデータの容量 36 等の情報を加えた暗号化データ 37 を生成する。また、本総合データ配信サービスでは運用によりこの暗号化データ 37 を、暗号化を行わないメタデータ 38 に再度埋め込み配信する場合と、別ファイルとして配信する場合とが可能である。図 51 に、本総合データ配信サービスにおいてコンテンツ、前述した各メタデータを暗号化する際に使用する暗号鍵、暗号鍵についての説明図を示す。

【0.02.5】(限定受信方式) 図 7 に、総合データ配信サービスにおける限定受信方式の説明図を示す。次に、本総合データ配信サービスにおいて有料放送等のコンテンツを放送事業者と契約のあるユーザーにのみ受信/蓄積させる限定受信の方式について図 7 を用いて説明する。本総合データ配信サービスにおける限定受信方式とは、従来のデジタル放送で使用される方式による端末毎にチャンネル単位、番組単位に行う方式とは異なり、メタデータを利用することにより端末を利用するユーザー毎に、コンテンツ単位の限定受信を可能とする。コンテンツ単位とは前述の通り、放送事業者の意図する単位であるため最小単位はエレメント単位となり、番組を構成するワンシーン等の細かい単位での限定受信が可能となる。本総合データ配信サービスにおける方式は、事前契約用メタデータ、鍵配信メタデータにより限定受信を行う。

【0026】まず受信側 200 のユーザーが有料事業者に対し端末 ID、個人 ID、契約したいチャンネル、番組、コンテンツ等の契約要求 39 を送出側 100 に通知する。送出側 100 ではユーザーより通知された契約要求より事前契約用メタデータを生成し、契約情報等の保護の必要な部分を受信端末毎に固有の端末鍵 Kmc で暗号化を行い受信側 200 にユーザー毎に配信する 45。受信側 200 の受信端末では、事前契約用メタデータ 40 の非暗号化部分に格納されている端末 ID、個人 ID により端末を使用するユーザー宛の情報かを判断し、使用ユーザー宛の ID が格納されている場合は、端末内に予め格納されている端末鍵 Kmc 43 により事前契約用メタデータを復号し、有料事業者 ID、事業者毎に固有の事業者鍵 Kw 44、契約コード等により構成される契約情報を入手する。契約情報を入手したユーザーは、次に契約事業者の放送するコンテンツ 17 の要求 46 を行う。送出側 100 では、暗号化コンテンツ 17 の配信と同期させコンテンツを視聴する際に必要となるコンテンツの暗号鍵 Kk 3

3 が格納され、必要部分を事業者鍵 Kw 44 で暗号化された鍵配信メタデータ 41 を全端末に配信する。また、送信側 100 では、コンテンツに対する利用制限情報等が格納され、必要部分がコンテンツ鍵 Kk 33 で暗号化された蓄積/再生用メタデータ 42 を全端末に配信する。

受信端末はコンテンツと同時に配信されている鍵配信メタデータ 41 を受信し、非暗号化部分に格納されている有料事業者 ID により契約事業者による放送かを判断し、契約する事業者の放送するコンテンツに対する鍵配信メタデータ 41 であると判断した場合、事前契約用 40 メタデータにより配信された事業者鍵 Kw により暗号化部分を復号し、復号された対象契約コードと事前契約用メタデータ 40 により配信された契約コードによりユーザーの契約形態内で利用可能なコンテンツかを判断する。ここで、利用可能であればコンテンツ鍵 Kk 33 を受信端末に格納し、同時に受信した蓄積/再生用メタデータ 42 の暗号化部分をコンテンツ鍵 Kk 33 により復号し、コンテンツに対する年齢制限等の利用制限情報を確認し、ユーザーの利用が可能であれば、蓄積/再生用メタデータ 42 に格納されている暗号化コンテンツ 17 の配信場所の情報により暗号化コンテンツ 17 の受信が可能となる。本総合データ配信サービスでは上記の方式により限定受信を可能とする。

#### 【0027】2. 課金方式

次に本総合データ配信サービスにおける課金方式について説明する。本総合データ配信サービスでは、事前契約に対する課金と、コンテンツの視聴時に対する課金の大きく 2 通りに分けられる。

【0028】(事前契約に対する課金) 図 8 に、事前契約による課金方式の説明図を示す。まず事前契約に対する課金について図 8 を用いて説明する。事前契約に対する課金とは、送出側 100 で予めユーザー登録 47 により得た顧客情報を元に課金を行うため、ユーザーのコンテンツ視聴の有無に関係せずに定額の課金が可能となる課金方式である。受信端末 3 を購入したユーザーは、送出側 100 に対し、端末 ID、個人 ID、契約したい事業者、契約形態、契約期間等の情報と共に決済先の銀行口座等 48 の情報を葉書や電話等により通知する。送出側 100 ではこれらの情報を元に顧客情報を生成管理し、契約した事業者の鍵、契約形態を示す契約コード、契約の有効期限等を格納した事前契約用メタデータ 40 を生成し契約ユーザーの受信端末 3 に向け配信し、ユーザーの指定した口座等 48 より一定期間のコンテンツ利用契約に対する課金を行う。事前契約メタデータ 40 を受信したユーザーは、格納されている有効期限の範囲で契約した事業者のコンテンツの利用が可能となる。以上が本総合データ配信サービスにおける事前契約に対する課金フローである。

【0029】(視聴契約に対する課金) 次に視聴契約に対する課金について説明する。本総合データ配信サービ



スにおける視聴契約に対する課金方式では、地上回線等の受信端末より送出側の上り回線を前提とした課金方式と、上り回線を前提としない課金方式に分けられる。

【0030】（上り回線を前提としない課金方式）図9に、上り回線を必要としない視聴契約に対する課金方式の説明図を示す。まず地上回線等の上り回線を前提としない課金方式について図9を用いて説明する。上り回線を前提としない課金方式とは、一定ポイントの利用料を事前契約の場合と同様に事前に支払い、そのポイントの範囲でコンテンツの視聴を行う方式である。但し、一定ポイントを超える場合は追加ポイントをその都度契約可能とする。具体的な手段としては、事前契約に対する課金と同様に、受信端末を購入したユーザーが端末ID、個人ID、契約したい事業者、契約形態、決済先の銀行口座48等を送出側100に通知し契約を行う際に一定期間に対する契約ではなく、コンテンツを利用するためのポイント数49を通知し契約を行う。送出側100では、これらの情報を元に顧客情報を生成管理し、契約の有効期限に関する情報の代わりに許諾するポイント数の情報を事前契約用メタデータ40に格納し契約ユーザーの受信端末3に配信する。また送出側100ではコンテンツ17を配信する際に同期させ配信させる蓄積/再生用メタデータ42にコンテンツを利用する際に必要となるポイント数の情報を格納し配信する。受信端末3ではコンテンツを利用する際に、事前契約用メタデータ40により配信されたポイント数より蓄積/再生用メタデータ42に格納されている必要ポイント数を減算し、コンテンツの再生を行うため、事前契約用メタデータ40で配信されたポイント数の範囲でのコンテンツの視聴が可能となる。事前契約用メタデータ40で配信されたポイント数がなくなった場合、ユーザーは再度送出側100と契約し、事前契約用メタデータ40を受信することによりポイントの補充が可能となる。送出側では、ユーザーに許諾したポイント数に応じて事前に通知された指定口座等48よりの課金が行えるため、ユーザーのコンテンツの視聴に応じた課金が可能となる。事前契約用メタデータ40により配信されるポイント数は、基本的にICカード内に格納するが、受信端末を利用するユーザーグループに対するポイント等の場合においては受信端末内に格納することも可能である。

【0031】（上り回線を前提とした課金方式）次に地上回線11等の上り回線を受信端末3に接続することを前提とした課金方式について説明する。本総合データ配信サービスにおける前項のポイントに対する課金方法の拡張として、ポイントの申し込み、ポイント追加等を受信端末3に接続された地上回線11等によりオンラインで可能にする方式と、実際に受信端末側でコンテンツを利用した際の課金情報50が送出側100に地上回線11等を通じて送られ、その情報を元に課金を行う方式が存在する。

【0032】図10に、上り回線を使用したオンライン課金方式の説明図を示す。ここでは後者の課金情報50による方式について図10を用いて説明する。オンラインで課金情報50を送出側100に送り課金を行うための具体的な手段としては、前述した課金方式と同様に受信端末3を購入したユーザーが端末ID、個人ID、契約したい事業者、契約形態、決済先の口座48等を送出側100に通知する際に、一定期間、一定ポイント数に対する契約ではなく、オンラインでのコンテンツの視聴に対する課金情報50を送るための契約を行う。本総合データ配信サービスでは、この契約をオンラインPPV許諾契約と呼ぶ。送出側100ではこれらの情報を元に顧客情報を生成管理し、契約の有効期限、許諾ポイント数等の情報の代わりにオンラインPPV許諾として、課金情報送信時の送信先の情報等を事前契約用メタデータ40に格納し契約ユーザーの受信端末3に配信する。また送出側100ではコンテンツ17を配信する際に同期させ配信させる蓄積/再生用メタデータ42にコンテンツを利用する際に必要となる利用時の料金などの課金情報50を生成する元となる情報を格納し配信する。受信端末ではコンテンツを利用する際に、蓄積/再生用メタデータ40に格納された課金情報50を生成するための元となる情報に対し利用ユーザーのID等の情報を加え、事前契約用メタデータ40により指定された送信先に対し地上回線を利用し送信する。これにより送出側100では契約ユーザーの受信端末3より送信された課金情報50内の料金を事前に登録された指定口座等48よりユーザーのコンテンツ視聴量に応じ課金可能となる。

### 【0033】3. サービスフロー

図11に、総合データ配信サービスにおけるサービスの流れの説明図を示す。次に本総合データ配信サービスにおけるサービスの流れについて図11を用いて説明する。本総合データ配信サービスは、例えば、受信端末3購入時に添付される葉書もしくは電話等を利用したユーザー登録時の事前契約フロー105、送出側100におけるコンテンツ生成102、メタデータ生成103から配信104までの送出側フロー101、コンテンツの受信、再生等の受信側フロー331を含む。

【0034】（事前契約フロー）図12に、事前契約におけるサービスフローの説明図を示す。以下に、事前契約におけるサービスフローを図12を用いて説明する。総合データ配信サービスにおける事前契約フロー105とは、送出側100におけるサービス受信ユーザー106の顧客情報管理107を行うことを目的とする。総合データ配信サービスでは有料の蓄積型コンテンツをメインとしたサービスであるため、ユーザーはコンテンツの視聴契約を行うためのICカード15が必要となり、そのICカード15をユーザーが取得する手段が事前契約である。前述の限定受信方式、課金方式で説明した通り、受

信側200のユーザー106は、端末購入時に添付され

る葉書もしくは電話等によりユーザー 106 の氏名、住所、有料放送視聴時等の決済先である銀行口座等のユーザー個人に関する個人情報および、視聴したい有料サービス、契約形態等を端末ID等の受信端末を識別する情報と共に送出側 100 に登録する。送出側 100 では、ユーザー登録された個人情報、契約情報、受信端末 3 を識別するための端末ID等の情報を元にユーザーに対し個人IDを割り振り顧客情報を生成管理 107 する。また、送信側 100 では、この顧客情報を元にICカード 15 に対し割り振った個人ID等の情報を格納し、ユーザー 106 に対しそれを配布し、受信端末 3、配布したICカード 15 に対してICカードを有するユーザー 106 が契約を行った事業者の鍵、契約形態を示す契約コード等の情報が格納された事前契約用メタデータ 40 を配信する。ユーザー 106 は契約したコンテンツの利用が可能となり、送出側 100 では契約ユーザーの顧客情報の管理が可能となる。

【0035】（送出側フロー）図 13 に、送出側におけるサービスフローの説明図を示す。以下に、送出側のサービスフローについて図 13 を用いて説明する。総合データ配信サービスにおける送出側のサービスフローとは、例えば、コンテンツの生成 102、番組編成 208、コンテンツの暗号化 209、配信フォーマット化 212、PSI/SI 生成 210、メタデータ生成 103、メタデータ暗号化 211、配信 104 を含む。

【0036】コンテンツ生成 102 とは、映像/音声/データの各エレメントよりコンテンツ 1 を生成することである。番組編成 208 とは、生成したコンテンツの 1 つあるいは複数を組み合わせるにより放送番組を制作することである。コンテンツの暗号化 209 は、番組化した各コンテンツに含まれるエレメントをコンテンツ毎の鍵であるコンテンツ鍵 Kk により暗号化し暗号化コンテンツ 17 を生成することである。配信フォーマット化 212 は、暗号化コンテンツ 17、暗号化されたメタデータをエレメントの種別により配信時のデータフォーマットであるTSP化することである。PSI/SI 生成 210 とは、番組編成 208 を行うことにより生成される番組の運行情報等を元にPSI/SIテーブル 19 を生成することである。メタデータ生成 103 とは、コンテンツ生成 102、番組編成 208 時のコンテンツ、番組に対するタイトル、内容、構成、利用制限情報等や、コンテンツ暗号化 209 における暗号方式、暗号鍵等の情報、配信フォーマット化 212 した際の伝送路における配信位置等の情報よりメタデータリスト 250、EPG用メタデータ 251、蓄積/再生用メタデータ 252、鍵配信用メタデータ 253 の各メタデータを生成することである。メタデータ暗号化 211 とは、メタデータ生成 103 により生成された各メタデータの保護が必要な部分に対し暗号化を行うことで、暗号化EPG用メタデータ 254、暗号化蓄積/再生用メタデータ 255、暗号化鍵配信用メタ

データ 256 を生成することである。配信 212 とは、PSI/SI、各メタデータ、暗号化コンテンツを多重化し受信側に配信することである。

【0037】（受信側フロー）図 14 に、受信側におけるサービスフローの説明図を示す。総合データ配信サービスにおける受信側のサービスフローとは、例えば、予約 332、コンテンツ受信/蓄積 333、視聴契約 334、再生 335 を含む。予約 332 とは、送出側 100 より配信されるEPG用メタデータ 254 を利用し、希望するコンテンツの予約を行うことである。コンテンツ受信/蓄積 333 とは、予約した情報を元にコンテンツ配信時刻に蓄積/再生用メタデータ 255、鍵配信用メタデータ 256、暗号化コンテンツ 17 を受信し、蓄積/再生用メタデータ 255、暗号化コンテンツ 17 を蓄積することである。視聴契約 334 とは、蓄積された蓄積/再生用メタデータの利用制限情報、ICカード 15 内の個人情報、契約情報等によりコンテンツの視聴契約を行うことである。再生 335 とは、視聴契約を行った情報をもとにコンテンツの再生許可等を判断し、暗号化コンテンツ 17 の復号を行った後、コンテンツの再生を行うことである。

#### 【0038】4. 送出側システム

次にこれらのサービスフローを実現させるための送出側のシステムについて説明する。

##### 送出側システム構成

図 15 に、送出側システム全体の構成図を示す。総合データ配信サービスにおける送出側システムの全体構成を図 15 を用いて説明する。送出側システムは前述の通りコンテンツやメタデータの生成、暗号化、配信を行う配信センタ 220、総合データ配信サービスシステムで使用する鍵や、IDを生成管理する鍵管理センタ 240、ユーザー登録情報により各ユーザーの個人情報、契約情報等の顧客情報の生成管理を行う顧客管理センタ 260、ユーザーからの視聴履歴情報/課金情報、リクエスト等の双方向通信サービス利用時の地上回線 11 による接続の管理を行う地上回線管理センタ 214、ユーザーや、販売店に対する商品等の配送など流通網 12 を利用した物流の管理を行う物流管理センタ 213 等を備える。本発明では総合データ配信サービスを実現する上で特に重要となる配信センタ 220、鍵管理センタ 240、顧客管理センタ 260 について詳細に説明する。

##### 【0039】（1）配信センタ構成

図 16 に、配信センタ内の構成図を示す。配信センタ 220 内の構成を図 16 を用いて説明する。配信センタ 220 はコンテンツの制作を行うオーサリングシステム 221、オーサリングシステム 221 で制作されたコンテンツより番組を編成し、運行スケジュール等を生成管理する番組構成管理システム 222、オーサリングシステム 221、番組構成管理システム 222 よりのコンテンツ生成時、番組編成時に生成されるコンテンツ及び番組

のタイトル、構成等の情報を元に各メタデータを生成するメタデータ生成装置 223、番組構成管理システム 222 で生成される運行スケジュール等を元に PSI/SI を生成する PSI/SI 生成装置 224、番組構成管理システム 222 により番組編成されたコンテンツ内の各エレメントを暗号化するコンテンツ暗号化装置 225、メタデータ生成装置 223 により生成されたメタデータの暗号化を行うメタデータ暗号化装置 226、PSI/SI 装置 224、コンテンツ暗号化装置 225、メタデータ暗号化装置 226 等より入力された情報を多重化し配信可能なフォーマットに変換する送出系システム 227 を備える。以下これら各構成について説明する。

【0040】（オーサリングシステム）図 17 に、オーサリングシステム内の構成図を示す。コンテンツを生成するオーサリングシステム 221 について図 17 を用いて説明する。オーサリングシステム 221 とはコンテンツ 1 の生成および管理を行い、完成したコンテンツ、コンテンツを生成する際に生成されるコンテンツに関するタイトル、内容、コンテンツ内の構成等の情報が格納された関連ファイル 233 を番組構成管理システム 222 に受け渡すシステムである。オーサリングシステム 221 の構成としては、映像、音声、データのエレメントを制作編集する映像オーサリングツール 228、音声オーサリングツール 229、データオーサリングツール 230、各オーサリングツールより出力されるエレメントよりコンテンツ 1 を構成し、関連ファイル 233 を生成するコンテンツ構成装置 231、コンテンツ構成装置により生成されたコンテンツ、関連ファイル 233 を蓄積管理するためのコンテンツ管理サーバ 232 を備える。

【0041】映像オーサリングツール 228、音声オーサリングツール 229、データオーサリングツール 230、の各オーサリングツールは、VHS ビデオ、レーザーディスク（登録商標）、写真等のアナログの素材入力 234 に対しデジタル化するビデオキャプチャ、スキャナ等の機能、DAT、CD、DVD 等のデジタルの素材入力 234 に対して受信側の受信端末が表示可能なフォーマットへの変換機能、各デジタル素材の編集機能、コンテンツ構成装置 231 に対して制作、編集を行った各エレメントのデジタル出力機能等を有する。コンテンツ構成装置 231 は、各オーサリングツールより出力される 1 つあるいは複数エレメントよりコンテンツ 1 を構成し、同時にコンテンツ名、コンテンツ ID、コンテンツの内容、ジャンル、コピー制限、対象年齢、著作権等の利用制限情報、構成するエレメントのデータ形式、容量等の情報を入力することにより関連ファイル 233 を生成しコンテンツ管理サーバ 232 に蓄積する機能を有する。コンテンツ管理サーバ 232 は、コンテンツの完成を番組構成管理システム 222 に対し通知し、番組構成管理システム 222 よりコンテンツ、関連ファイル 233 の転送要求が起こった場合、番組構成管理システム 222 に対し

要求されたコンテンツ 1、関連ファイル 233 を受け渡す機能を有する。但し、コンテンツ管理サーバ 232 は番組構成管理システム 222 より転送要求が無い場合においても強制的に番組構成管理システムに対しコンテンツ 1、関連ファイル 233 を受け渡す機能をも有する。

【0042】（番組構成管理システム）図 18 に、番組構成管理システム内の構成図を示す。次に番組構成管理システム 222 について図 18 を用いて説明する。番組構成管理システム 222 とは、オーサリングシステム 221 で生成されたコンテンツより番組を構成し、構成した番組に対する運行スケジュール等を生成管理することにより番組を編成するシステムである。番組構成管理システム 222 は、オーサリングシステム 221 内のコンテンツ管理サーバ 232 より入力されるコンテンツ 1 より番組を構成する番組構成装置 235、構成された番組に対し運行スケジュール 238 を生成し、割り当てる番組運行スケジュール生成装置 236、番組化されたコンテンツ群、それに対応する関連ファイル群、運行スケジュールを蓄積管理する番組管理サーバ 237 を備える。なお、図 17、18 のコンテンツ生成におけるコンテンツに関連する情報を纏めたファイルをコンテンツ関連情報と総称し、それを記憶したファイルが関連ファイル 233 である。

【0043】番組構成装置 235 とは、コンテンツ管理サーバ 232 より 1 つあるいは複数のコンテンツ 1、関連ファイル 233 より番組を構成し、番組としてのコンテンツ群、番組に対する情報、例えば番組のタイトル、番組の ID、番組の内容、ジャンル、放送する事業者の ID、契約に関する情報、課金に関する情報、番組内におけるコンテンツの構成等の情報をコンテンツ管理サーバ 232 より入力された関連ファイル 233 に追加し、番組管理サーバ 237 に対し蓄積する機能を有する。番組運行スケジュール生成装置 236 は、番組管理サーバ 237 に蓄積された番組に対し、放送日時、チャンネル等の放送場所に関する情報等を割り当て、運行スケジュール 238 を生成し番組管理サーバ 237 に蓄積する機能を有する。番組管理サーバ 237 は、番組構成装置 235、番組運行スケジュール生成装置 236 より入力されたコンテンツ群 1、関連ファイル群 233、運行スケジュール 238 等を蓄積管理し、運行スケジュール 238 の情報を元に、メタデータ生成装置 223、PSI/SI 生成装置 224 に対し運行スケジュール 238、関連ファイル群 233 を入力し、コンテンツ暗号化装置 225 に対しメタデータ生成装置 223、PSI/SI 生成装置 224 に入力した番組情報に対応するコンテンツ群及びコンテンツの ID 群を入力する機能を有する。

【0044】（PSI/SI 生成装置）図 19 に、PSI/SI 生成装置の説明図を示す。PSI/SI 生成装置 224 について図 19 を用いて説明する。PSI/SI 生成装置 224 とは、番組構成管理システム 222 内の番組管理サーバ 237 より

り入力される運行スケジュール 238、関連ファイル群 233よりMPEG2-Systemに準拠したPSI/SIの各テーブルを生成し、運行スケジュールの情報を元に送出系システム 227に対しTSP化した各PSI/SIテーブルを入力する機能を有する。

【0045】(メタデータ生成装置)図20に、メタデータ生成装置の説明図を示す。次にメタデータ生成装置 223について図20を用い説明する。メタデータ生成装置 223とは、番組構成管理システム 222内の番組管理サーバ 237より入力される関連ファイル群、運行スケジュール、鍵管理センタ 240に対しコンテンツのIDを受け渡すことにより得られるコンテンツ鍵Kk、送出系システム 227より入力されるコンテンツ等の伝送路における配信位置情報等を元に、メタデータリスト 250、EPG用メタデータ 251、鍵配信用メタデータ 253、蓄積/再生用メタデータ 252を生成し、メタデータリストを送出系システム 227に出力し、その他のメタデータをメタデータ暗号化装置 226に出力する機能を有する。送出系システムより入力されるコンテンツ等の伝送路における配信位置情報は、送出系システム 227側の装置により配信位置であるモジュールの指定等が可能であれば必要としない場合もある。

【0046】(コンテンツ暗号化装置)図21に、コンテンツ暗号化装置の説明図を示す。本システムにおけるコンテンツ暗号化装置 225について図21を用いて説明する。コンテンツ暗号化装置 225とは、番組構成管理システム 222内の番組管理サーバ 237より入力されるコンテンツ群、ID(コンテンツID)群に基づき、番組管理サーバ 237より入力されたID(コンテンツID)を鍵管理センタ 240に通知し、該当するコンテンツ鍵Kkを受け取り、また、コンテンツ鍵Kkにより対応するコンテンツ内の各エレメントを前述のコンテンツ暗号化方式の通り暗号化し、生成した暗号化コンテンツを送出系システム 227に対し出力する機能を有する。

【0047】(メタデータ暗号化装置)図22に、メタデータ暗号化装置の説明図を示す。次にメタデータ暗号化装置 226について図22を用い説明する。メタデータ暗号化装置 226とは、メタデータ生成装置 223より入力されるEPG用メタデータ 251、蓄積/再生用メタデータ 252、鍵配信用メタデータ 253、顧客管理センタ 260より入力される事前契約用メタデータ 259を鍵管理センタ 240内より入力される暗号鍵情報により暗号化し、生成された暗号化メタデータを送出系システム 227に対し出力する機能を有する。

【0048】各メタデータの暗号化方式について、以下に説明する。EPG用メタデータ 251については、鍵管理センタ 240に対しEPG用メタデータ 251に格納されたシステムIDを受け渡すことにより得られる全受信端末に共通したシステム鍵Ksy 264により必要部分に対し暗号化が行われる。蓄積/再生用メタデータ 252に

については、鍵管理センタ 240に対し蓄積/再生用メタデータ 252に格納されたコンテンツIDを受け渡すことにより得られるコンテンツ毎に固有のコンテンツ鍵Kk 33により必要部分に対し暗号化が行われる。鍵配信用メタデータ 253については、メタデータ内に格納されているIDを次のように暗号化する。すなわち、無料コンテンツに対する鍵配信用メタデータ 257であれば、システムIDを、鍵管理センタ 240に受け渡すことにより得られるシステム鍵Ksy 264により、必要部分に対し暗号化する。また、有料コンテンツに対する鍵配信用メタデータ 258であれば、事業者IDを、事業者鍵Kw 44により、それぞれ必要部分に対し暗号化する。事前契約用メタデータ 259については、鍵管理センタ 240に対し事前契約用メタデータ 259内に格納された端末IDを受け渡すことにより得られる端末鍵Kmc 43により必要部分に暗号化が行われる。

【0049】よって送出系システム 227に対しては生成された暗号化EPG用メタデータ 254、暗号化蓄積/再生用メタデータ 255、暗号化鍵配信用メタデータ(無料) 261、暗号化鍵配信用メタデータ(有料) 262、暗号化事前契約用メタデータ 263が出力されることとなる。

【0050】(送出系システム)図23に、送出系システム内の構成図を示す。以下に、総合データ配信サービスにおける送出系システム 227について図23を用いて説明する。送出系システム 227とは、PSI/SI生成装置 224、コンテンツ暗号化装置 225、メタデータ暗号化装置 226、メタデータ生成装置 223より入力されるPSI/SI、暗号化コンテンツ、メタデータ等のデータを、受信端末 3に対し配信可能なデータに組み立てるシステムである。送出系システム 227は、カラーセル生成装置 239、パケタイザ 241、多重化装置(MUX) 242、受託放送設備 243を備える。カラーセル生成装置 239とは、コンテンツ暗号化装置 225より入力されるデータ系の暗号化コンテンツ、メタデータ暗号化装置より入力される暗号化された各メタデータ、メタデータ生成装置より入力されるメタデータリストよりMPEG2-systemにおけるデータカラーセルを生成するために各データをモジュール化したのちDII、DDB化し、パケタイザ 241に対し出力する機能を有する。パケタイザ 241とは、コンテンツ暗号化装置より入力されるMPEG2-Video PES、MPEG2-Audio PES等の映像系の暗号化コンテンツ、カラーセル生成装置より入力されるDII、DDB等のデータをTSP形式のデータに分割し多重化装置(MUX) 242に対し出力する機能を有する。多重化装置(MUX) 242とは、PSI/SI生成装置 224、パケタイザ 241より入力されるTSPに対し送出レート等の条件により多重化を行いTSを生成し、受託放送設備 243に出力する機能を有する。受託放送設備 243とは、多重化装置(MUX) 242より入力される複数TSをさらに多重化し、受

信端末 3 に対して配信可能なデータ形体とし送信アンテナより配信を行う機能を有する。以上が本総合データ配信サービスにおける配信センタ 220 内の構成および各構成装置の機能及びデータ生成フローである。

#### 【0051】 (2) 鍵管理センタ構成

図 24 に、鍵管理センタ内の構成図を示す。次に鍵管理センタ 240 について図 24 を用いて説明する。鍵管理センタ 240 とは、配信センタ 220、顧客管理センタ 260 より登録される各 ID に対する暗号鍵を生成し、各センタからの暗号鍵の要求に対して暗号鍵を受け渡すシステムである。鍵管理センタ 240 は、鍵生成装置 244、鍵管理サーバ 245 を備える。

【0052】 (鍵生成装置) 図 25 に、鍵生成装置の説明図を示す。次に鍵管理センタ 240 における鍵生成装置 244 について図 25 を用いて説明する。鍵生成装置 244 とは、配信センタ 220 内のメタデータ生成装置 223 より入力される複数のコンテンツ ID 246 よりそれぞれの ID に対応するコンテンツの暗号鍵であるコンテンツ鍵 Kk 33 を生成し、生成したコンテンツ鍵 Kk 33 をコンテンツ ID 246 と共に鍵管理サーバ 245 に対し出力する機能を有する。また、システム鍵 Ksy 264、事業者鍵 Kw 44、端末鍵 Kmc 43、個人鍵 Km 265 については鍵生成装置 244 内で各暗号鍵に対する ID であるシステム ID 247、事業者 ID 248、端末 ID 249、個人 ID 270 を直接指定することにより生成し、各 ID と共に鍵管理サーバ 245 に対し出力する。

【0053】 (鍵管理サーバ) 図 26 に、鍵管理サーバの説明図を示す。次に鍵管理サーバ 245 について図 26 を用いて説明する。鍵管理サーバ 245 とは、鍵生成装置 244 により生成された鍵及び ID を管理し、配信センタ 220 内のコンテンツ暗号化装置 225、メタデータ暗号化装置 226、メタデータ生成装置 223、顧客管理センタ 260 内の顧客情報管理サーバ 267 からの暗号鍵の要求に対し対応する暗号鍵を受け渡す機能を有する。例えば配信センタ 220 内のコンテンツ暗号化装置 225 より暗号鍵の要求としてコンテンツ ID を受け渡された場合は、コンテンツ ID に対応する暗号鍵であるコンテンツ鍵 Kk を受け渡す機能である。

#### 【0054】 (3) 顧客管理センタ構成

図 27 に、顧客管理センタ内の構成図を示す。次に本総合データ配信サービスシステムにおける顧客管理センタについて図 27 を用いて説明する。顧客管理センタ 260 とは、ユーザー 106 からのユーザー登録情報を元に顧客情報を生成し、鍵管理センタ 240 より受け渡される暗号鍵等の情報により IC カード、事前契約用メタデータを生成し、IC カードをユーザー 106 に配布し、事前契約用メタデータを配信センタ 220 に受け渡すシステムである。顧客管理センタ 260 は、顧客情報生成システム 266、顧客情報管理システム 271 を備える。

【0055】 (顧客情報生成システム) 図 28 に、顧客

情報生成システム内の構成図を示す。顧客管理センタ 260 における顧客情報生成システム 266 について図 28 を用いて説明する。顧客情報生成システム 266 とは、ユーザー 106 が端末購入時に添付される葉書もしくは電話にて事前契約等のユーザー登録を行った情報より顧客情報を生成し、顧客情報管理システム 271 に対し出力するシステムであり、ユーザー I/F 268、顧客情報生成装置 269 を備える。ユーザー I/F 268 とは、ユーザーからの葉書、電話等によるユーザー登録情報を受け、登録された情報を電子化する機能を有する。顧客情報生成装置 269 とは、ユーザー I/F 268 により電子化されたユーザー登録情報を顧客情報管理システム 271 が認識可能なデータ形式である顧客情報に編集し、顧客情報管理システム 271 に対し出力する機能を有する。

【0056】 (顧客情報管理システム) 図 29 に、顧客情報管理システム内の構成図を示す。顧客情報管理システム 271 とは、顧客情報生成システム 266 により入力される顧客情報を元に鍵管理センタ内の鍵管理サーバ 245 に対し個人 ID 270、個人鍵 265 等を要求し、受け取った個人 ID 270、個人鍵 265 等を利用し、事前契約用メタデータ 40、IC カード 15 等を生成するシステムである。顧客情報管理システム 271 は、顧客情報管理サーバ 267、IC カード生成装置 272、事前契約用メタデータ生成装置 273 を備える。

【0057】 顧客情報管理サーバ 267 とは、顧客情報生成システム 266 で生成された顧客情報の管理を行い、鍵管理サーバ 245 より個人鍵 Km 265、ユーザーが契約を行う事業者鍵 Kw 等の情報を受け取るためのユーザー情報 150 を生成し、鍵管理サーバ 245 に対し出力する。ユーザー情報 150 とは、例えば、ある端末 ID の振られた受信側の受信端末に対し何人のユーザーが利用するか、また端末を利用するユーザーがどの放送事業者と契約を行うかを示した情報である。このユーザー情報 150 により鍵管理サーバ 245 は、管理する個人 ID 270/個人鍵 Km 265 をユーザー情報に格納されているユーザー数分確保し、同じくユーザー情報に格納されている端末 ID 249 に対応する端末鍵 Kmc 43、各ユーザーが契約を行う事業者 ID に対応する事業者鍵 Kw を顧客情報管理サーバ 267 に受け渡すことが可能となる。顧客情報管理サーバ 267 は受け取った個人 ID 270、個人鍵 Km 265、端末 ID 249、端末鍵 Kmc 43、事業者 ID、事業者鍵 Kw を顧客情報に追加することによりユーザーの使用する端末、ユーザー自身の個人情報、契約情報等の把握が可能となり顧客管理が可能となる。IC カード生成装置 272 は、顧客情報管理サーバ 267 内の顧客情報をもとに空 IC カード内の所定エリアに個人 ID 270、個人鍵 Km 265、端末 ID 249、各ユーザーの名前、電話番号、生年月日等の個人契約情報を格納し各ユーザー 106 に配布する。事前契約用メタデータ生成装

置 273 とは、ICカード生成装置 272 と同様に顧客情報管理サーバ 267 内の顧客情報により各ユーザーの契約する事業者のID、事業者鍵Kw、契約形態を示す契約コードおよび、各ユーザーに割り振られた個人ID 270、各ユーザーが使用する受信端末のID 249 を格納した事前契約用メタデータを生成し配信センタ内のメタデータ暗号化装置 226 に受け渡す。以上が送出側システムの構成及び、各装置間のデータフローである。

【0058】（送出側で生成配信される情報）次に送出側で生成し、受信端末に対して配信される各メタデータについて説明する。本総合データ配信サービスにおけるメタデータの記述方式は、前述の図 6 におけるXML等のテキスト形式での記述、PSI/SIのようなバイナリ形式での記述が可能である。ただし、暗号化が必要な部分については受信端末内での記述内容解釈処理の向上の点で特にバイナリ形式での記述を行うが、受信端末の処理性能が高い場合は、非暗号化部分と同様にテキスト形式での記述による運用も可能である。各メタデータの記述内容、構成について説明する。

【0059】（事前契約用メタデータ）図 30 に、事前契約用メタデータの構成および格納される情報の説明図を示す。まず、事前契約用メタデータについて図 30 を用いて説明する。事前契約用メタデータ 263 とは、前述の通り有料放送事業者の事業者鍵Kwや、契約形態に間する契約コード等の内容を含み、主に限定受信を行う際の判定材料に利用されるデータであり、端末購入時、契約更新時、事業者鍵Kwの更新時等に配信されるメタデータである。端末ID、個人ID等の受信端末が端末を利用するユーザー宛に送られたデータかを識別するためのユーザー識別情報 275 と、メタデータの暗号方式、暗号化部分、暗号鍵を示すID（端末ID）等のメタデータにかけられた暗号に関する暗号化情報 276 と、ユーザーの名前、電話番号、住所、決済能力、決済先、パスワード等のユーザー自身の個人情報 277 と、ユーザーが契約を行う契約事業者のID、事業者鍵Kw、契約の有効期限、契約コード、契約ポイント等の契約情報 278 等を含む。暗号化部分については、各ユーザーの決済先等の情報が格納される個人情報 277、事業者鍵Kw等の情報が格納される契約情報 278 が該当し、ユーザーの利用する端末固有の鍵Kmc 43 により送出側で暗号化され、受信端末に配信される。暗号化に使用する暗号鍵については運用により個人鍵Kmを使用することも可能である。また、運用により事前契約用メタデータに上記の情報以外に後述するメタデータ属性情報が格納されることも可能である。

【0060】（EPG用メタデータ）図 31 に、EPG用メタデータの構成および格納される情報の説明図を示す。次に EPG用メタデータ 254 について図 31 を用いて説明する。EPG用メタデータ 254 とは、主にユーザーが配信予定コンテンツの確認、配信予定コンテンツの視聴/

蓄積予約を行うためのメタデータであり、EPG用メタデータの配信時が蓄積/再生用メタデータ、鍵配信用メタデータの配信時と重なるため各メタデータを識別するためのメタデータID、メタデータのタイプ、メタデータのサイズ等のメタデータ属性情報 279 と、事前契約用メタデータと同様にメタデータの暗号部分に関する暗号化情報 276 と、番組のID、放送予定日時、番組の内容、ジャンル、コンテンツの構成、番組のサイズ等の番組に関する番組情報 280 と、コンテンツのID、コンテンツの内容、エレメントの構成等のコンテンツ情報 281 と、コンテンツを利用するユーザー、コンテンツ自体に対する制限情報である年齢制限、コピー制限、蓄積制限等の利用制限情報 282 等を含む。暗号化部分についてはコピー制限等の利用制限情報 282 が該当し、全ユーザーのメタデータの利用を可能とするため、全受信端末共通のシステム鍵Ksy 264 により送出側で暗号化され配信される。コンテンツ情報 281 については、総合データ配信サービスにおける EPGの運用レベルにより格納せずに配信することも可能とする。利用制限情報についても同様に格納せずに運用を行う場合もあり、EPG用メタデータは暗号化せずに配信されることも可能である。

【0061】（蓄積/再生用メタデータ）図 32 に、蓄積/再生用メタデータの構成および格納される情報の説明図を示す。次に蓄積/再生用メタデータ 255 について図 32 を用いて説明する。蓄積/再生用メタデータ 255 とは、コンテンツの受信、蓄積、再生に必要な情報を含むメタデータであり、蓄積済みコンテンツの検索時に利用される他、ユーザーのコンテンツ利用方法を制御するために利用される。蓄積/再生用メタデータは、EPG用メタデータと同様にメタデータ自体を識別するためのメタデータ属性情報 279 と、暗号化情報 276 と、番組情報 280 と、コンテンツ情報 281 と、利用制限情報 282 と、蓄積/再生用メタデータが示すコンテンツの暗号化方式、暗号鍵ID等のコンテンツ暗号化情報、コンテンツを視聴するための契約に関する、契約形態、契約による利用可能期間等の契約情報 284 と、契約による課金料金、課金タイミング等の課金情報 285 等を含む。暗号化部分については利用制限情報 282、コンテンツの暗号化方式、暗号鍵ID等の情報が含まれるコンテンツ暗号化情報 283、使用制限期間等の情報が含まれる契約情報 284、課金時の料金、タイミング等が含まれる課金情報 285 が該当し、コンテンツを暗号化した鍵と同じコンテンツ鍵Kk 33 により送出側で暗号化され配信される。また、蓄積/再生用メタデータにおけるコンテンツ情報 281 については、EPG用メタデータ内に格納されるコンテンツ情報にコンテンツの配信位置等の情報が追加される。

【0062】（鍵配信用メタデータ）図 33 に、鍵配信用メタデータの構成および格納される情報の説明図を示す。次に鍵配信用メタデータ 256 について図 33 を用

いて説明する。鍵配信用メタデータ 256 とは、コンテンツの暗号鍵に関する情報を配信するためのメタデータであり、コンテンツが有料放送の場合は放送する事業者と契約したユーザーのみ受信可能とする限定受信を行うための情報が含まれる。鍵配信用メタデータ 256 は、他のメタデータより区別するためのメタデータ属性情報 279 と、メタデータ自体の暗号化に関する暗号化情報 276 と、コンテンツの ID、コンテンツの暗号鍵 Kk 等のコンテンツ鍵情報 286 等を含む。暗号化部分に関してはコンテンツ鍵 Kk 等のコンテンツ鍵情報が送出側で暗号化され配信される。暗号鍵については、鍵配信用メタデータ 256 が有料コンテンツに対するメタデータであり、事業者と契約したユーザーのみ受信可能な限定受信を行う場合は、事業者毎に固有の事業者鍵 Kw 44 が使用され、契約者以外のユーザーも視聴可能な無料コンテンツに対するメタデータの場合は、全受信端末に共通なシステム鍵 Ksy 264 が使用される。また、限定受信を実現させるための事業者 ID、対象契約コード等の情報はコンテンツ鍵情報に格納され暗号化されて配信される。

【0063】(メタデータリスト) 図 34 に、メタデータリストの構成および格納される情報の説明図を示す。次にメタデータリスト 250 について図 34 を用いて説明する。メタデータリストとは、配信ストリーム中の EPG 用メタデータ、蓄積/再生用メタデータ等の配信位置を取得するためのメタデータであり、PSI を補完する情報を持ち、受信端末内に蓄積した EPG 用メタデータに対し配信ストリーム中の EPG 用メタデータが更新された場合における差分メタデータ蓄積のための情報を含む。メタデータリスト 250 は、受信端末側で情報の更新を識別するためのバージョン等のメタデータリスト属性情報 287 と、コンテンツ ID に対応するメタデータの ID、EPG 用メタデータ、蓄積/再生用メタデータを区別するためのメタデータタイプ、EPG 用メタデータの更新を識別するためのメタデータのバージョン、配信ストリーム上の位置情報等のリスト情報 288 等を含む。メタデータリスト自体はメタデータを配信ストリームより取得するための情報であるため特に保護を必要とせず、暗号化は行わずに配信される。メタデータリストの取得方法としては PSI テーブルにおける PMT 内に配信ストリームを指定することにより取得を行う運用とする。

【0064】(システム鍵更新用メタデータ) 図 35 に、システム鍵更新用メタデータの構成および格納される情報の説明図を示す。次にシステム鍵更新用メタデータについて図 35 を用いて説明する。システム鍵更新用メタデータ 289 とは、受信端末内に格納されている全受信端末共通の鍵であるシステム鍵 Ksy をシステム鍵 Ksy 3 に更新するためのメタデータである。システム鍵更新用メタデータ 289 は、他のメタデータと区別するためのメタデータ属性情報 279 と、メタデータ自体の暗号化に関する暗号化情報 276 と、更新対象となるシステ

ム鍵に対応するシステム ID、変更後のシステム ID、システム鍵、更新タイミング等の情報が含まれるシステム鍵情報 290 等を含む。

【0065】暗号化部分は、更新後のシステム鍵、変更タイミング等の情報が含まれるシステム鍵情報 290 が該当し、暗号鍵は受信端末内に予め予備用のシステム鍵として登録されているシステム鍵 Ksy2 を使用する。システム鍵 Ksy は、システム鍵全体の総称で、通常は 1 つが有効である。ただし、ハック等の被害があった時に、予備のシステム鍵 Ksy2 を使用する。そのために、受信機には通常 2 つのシステム鍵 Ksy1、Ksy2 が内蔵されている。システム鍵 Ksy の更新処理を具体的に説明するために、システム鍵 Key の実際の受信機内の構成である 2 つシステム鍵 Key1、Key2 について述べる。Key1、Key2 が受信機内部に内蔵されており、これらの鍵を更新等の変更をする時に、システム鍵送信側は、他のシステム鍵 Key3 を衛星より伝送し、受信端末では、システム鍵 Ksy1 が Key3 に変更となる。これより実際の受信機内には、システム鍵 Key2、Ksy3 の 2 つの鍵が存在することになる。また、システム鍵 Key2 が実際には有効鍵となる。以上が本総合データ配信サービスにおける送出側より配信されるメタデータである。

#### 【0066】5. 受信側システム

つぎに、上述のサービスフローを実施させる受信側システムである受信端末について説明する。

(受信端末構成) 図 36 に、受信端末内の構成図を示す。次に本総合データ配信サービスにおける受信側である受信端末 3 について図 36 を用いて説明する。受信端末 3 は衛星を介したコンテンツ 17、PSI/SI 19、メタデータ 18 等の情報をアンテナ 2 により受信し、TV 9 等のモニタ装置に出力、また蓄積媒体 4 内に蓄積後出力することでユーザーの視聴を可能とする。将来的にはこの受信端末 3 が TV 9 等のモニタ装置に内蔵されることもあるがここでは一例として、別装置として説明する。総合データ配信サービス用の受信端末 3 の大きな特徴としては、コンテンツ 17 及びメタデータ 18 等の情報を蓄積するための蓄積媒体 4 を有している他に、暗号化し配信されたデータの復号及び受信端末内で生成される重要なデータに対し暗号化を行い、著作権保護等の権利、認証、課金等の処理、制御に関わる RMP 16 機能、この受信端末を利用するユーザーの個人認証、及びユーザーの属する家族等のグループ認証を行う個人認証デバイスである IC カード 15 を有していることである。この RMP 16 機能とは、メタデータの内容を解釈し権利保護に関わる処理の制御を行う RMP コントローラ 306、暗号化されたメタデータを復号するメタデータ復号機能 307、暗号化されたコンテンツを復号するためのコンテンツ復号機能 308、受信端末内で使用する鍵を管理する鍵管理テーブル 311、受信端末を利用するユーザーの環境を設定するためのプロファイル 310、受信端末内でメ



タデータ等より生成されるコンテンツの視聴を許諾する情報等の保護が必要なデータを暗号化するメタデータ暗号機能309等を含む。蓄積媒体4は、前述のコンテンツ17、メタデータ18の他に、受信端末内で生成される予約情報313、検索/EPGテーブル312等の情報が格納される受信端末に固定的な大容量蓄積媒体であるハードディスクや、必要なコンテンツ、メタデータ等の情報を格納する取り外し可能なDVD-RAM、メモリカード等のリムーバブルメディアを備える。ICカード15は、前述した個人ID270、個人鍵265、個人契約情報274の他に、受信端末内で生成されるコンテンツの視聴を許諾する判断材料となる許諾情報314等が格納される。RMP16については、パイレーツや暗号解読などに対するセキュリティ対策としセキュリティの守られた構成よりなるが、セキュリティ強度の退化等によりモジュールごと取り替えることが可能な構成も考えられる。

【0067】次に受信端末の特徴的な機能であるRMP16、蓄積媒体4、ICカード15について説明する。

(RMP) 本総合データ配信サービスにおけるRMP16機能とは、メタデータの内容を解釈し権利保護に関わる処理の制御を行うRMPコントローラ306、暗号化されたメタデータを復号するメタデータ復号機能307、暗号化されたコンテンツを復号するためのコンテンツ復号機能308、受信端末内で使用する鍵を管理する鍵管理テーブル311、受信端末を利用するユーザーの環境を設定するためのプロフィール310、受信端末内でメタデータ等より生成されるコンテンツの視聴を許諾する情報等の保護が必要なデータを暗号化するメタデータ暗号機能309等を含む。

【0068】図52に、RMPコントローラ306の行う主な制御処理について示す。RMPコントローラ306の主な機能としては、図示のように、例えば、受信制御、蓄積制御、コピー制御、提示制御、視聴契約制御、課金制御、個人認証制御、鍵管理、プロフィール管理、時刻管理、アプリケーション認証制御、外部機器認証制御、外部機器認証制御、通信回線制御がある。

【0069】(メタデータ復号) 図37に、メタデータ復号機能の説明図を示す。次にメタデータ復号について図37を用いて説明する。メタデータ復号機能307とは、RMPコントローラ306より復号要求が起こった際に、鍵管理テーブル311よりRMPコントローラ306を介して受け渡される暗号鍵を使用し、暗号化されたメタデータ等を復号する機能である。RMPコントローラ306は、コンテンツの受信/蓄積時、コンテンツの視聴契約時等でメタデータを復号する必要があると判断した場合、まず蓄積媒体内の暗号化されたメタデータもしくはICカード内の暗号化された個人契約情報等を複製し、各データの非暗号化部分に格納されている前述した暗号化情報内の暗号鍵IDを読み取り、暗号鍵IDを鍵管理テーブル311に受け渡す。鍵管理テーブル311は受け渡

された暗号鍵IDより対応する暗号鍵を識別し、RMPコントローラ306に対し暗号鍵を受け渡す。RMPコントローラ306は、鍵管理テーブルより受け渡された暗号鍵と、メタデータをメタデータ復号機能307に受け渡し、復号を要求する。メタデータ復号機能307は、受け渡されたメタデータの暗号部分を抽出し、抽出した暗号部分をRMPコントローラ306より同じく受け渡された暗号鍵により復号し、非暗号化部分のメタデータの所定部分に格納し、RMPコントローラ306に復号したメタデータとして受け渡す。ただし、復号したデータについては前述した通り運用により非暗号化部分とデータ形式が異なる場合があるため、その際は格納せずにその後の処理を行う運用を行うこともある。以上がメタデータ復号機能307の復号処理である。メタデータ復号機能307が復号するメタデータとは、EPG用メタデータ254、蓄積/再生用メタデータ255、鍵配信用メタデータ(無料)261、鍵配信用メタデータ(有料)262、事前契約用メタデータ263、システム鍵更新用メタデータ289の各メタデータの他に、ICカードに格納される個人契約情報274、許諾情報314が挙げられる。ICカード内の情報である個人契約情報274、許諾情報314については、暗号鍵が鍵テーブルに格納されていないため、ICカード内の個人鍵Km265をRMPコントローラ306より取得し復号を行う。

【0070】(コンテンツ復号) 図38に、コンテンツ復号機能の説明図を示す。コンテンツ復号について図38を用いて説明する。コンテンツ復号機能308とは、RMPコントローラ306の復号要求に対し、鍵管理テーブル311よりRMPコントローラ306を介し受け取ったコンテンツの暗号鍵であるコンテンツ鍵を使用し、コンテンツ17内の各エレメントを復号する機能であり、主にコンテンツの再生時に行われる処理である。

【0071】(プロフィール) 図39に、プロフィールの構成図を示す。次にプロフィールについて図39を用いて説明する。プロフィール310とは、事前契約用メタデータ263よりRMP内で生成される個人契約情報274の集合であり、保護の必要なデータであるため、RMP内部のセキュリティの守られた記憶エリア(セキュアメモリ)317に格納され、コンテンツの視聴/蓄積予約、限定受信の判定時等に使用される。プロフィール310は端末ユーザー全体に対する契約情報等の格納された全体プロフィール315と、各ユーザー毎の契約情報が格納された個人プロフィール316を含む。

【0072】(鍵管理テーブル) 図40に、鍵管理テーブルの構成図を示す。鍵管理テーブルについて図40を用いて説明する。鍵管理テーブル311とは、RMPコントローラ306より指定されるIDに対して該当する鍵を受け渡すための情報であるID及び鍵を格納したテーブルであり、保護の必要な鍵データより構成されるため、プロフィールと同様にRMP内部のセキュリティの守られた



記憶エリア（セキュアメモリ）317に格納される。

【0073】（メタデータ暗号）図41に、メタデータ暗号機能の説明図を示す。メタデータ暗号について図41を用いて説明する。メタデータ暗号機能309とは、RMP16よりICカード15に対し事前契約用メタデータより生成した個人契約情報274や、蓄積/再生用メタデータより生成したコンテンツの許諾情報314を格納する際に、各情報をICカード15内の個人鍵Km265を用いて暗号化する機能である。

【0074】（蓄積媒体）図42に、蓄積媒体内に格納される情報の蓄積状態の説明図を示す。次に受信端末3における蓄積媒体4に格納されるデータの蓄積状態について図42を用いて説明する。蓄積媒体4に格納されるデータとしては、メタデータリスト250、EPG用メタデータ254、検索/EPGテーブル312、予約情報313、蓄積/再生用メタデータ255、コンテンツ17、その他受信端末のOS、アプリケーション等のソフトウェア等が存在する。蓄積媒体4自体は、この例では、セキュリティの保護された構造ではないため、蓄積媒体内に格納されるデータにおいて保護の必要なデータは、暗号化状態で蓄積される。EPG用メタデータ254や蓄積/再生用メタデータ255等を受信するためのメタデータリスト250と、EPG用メタデータ254や蓄積/再生用メタデータ255より生成され、受信端末のEPG表示、検索処理を行うための検索/EPGテーブル312と、EPG用メタデータ254より生成されるコンテンツ視聴/蓄積予約のための予約情報313とは特に保護の必要とされないデータであるため暗号化せずに蓄積媒体に格納される。ただし運用において保護が必要な場合は、端末内に予め存在する端末鍵Kmc等により暗号化を行う。コンテンツの利用制限情報等が格納されたEPG用メタデータ254、蓄積/再生用メタデータ255、コンテンツ17については送出側で暗号化された状態で蓄積され、各データが処理に必要な際はコピーを生成し、コピーを復号し利用することにより受信端末内での再暗号化処理を省くことが可能となる。

【0075】（ICカード）図43に、ICカード内の構成の説明図を示す。総合データ配信サービスにおいて利用されるICカード15内の構成について図43を用いて説明する。ICカード15内は、セキュリティの守られた記憶エリア（セキュアメモリ）317と通常の記憶エリア（通常メモリ）318を備える。通常の記憶エリア318では、保護の必要でないデータもしくは、保護が必要であるが暗号化することで保護されているデータが格納され、一方、セキュリティの守られた記憶エリア317に格納される情報は保護が必要なデータであるがICカード内で暗号化状態で保存できない情報が格納される。セキュリティが守られた記憶エリア317に格納される情報としては、ユーザー個人に割り当てられた個人ID270、それに対応する暗号鍵である個人鍵Km265等が該

当し、一方、通常の記憶エリア318に格納されるデータは、RMP16側で暗号化された個人契約情報274、許諾情報314等が該当する。また、セキュリティの守られた記憶エリア317に格納された個人ID270、個人鍵265をRMP16に受け渡す場合は、同じくセキュリティの守られた伝送路を使用し、データの受け渡しを行う。セキュリティの守られた伝送路とは、公開鍵方式等を利用することにより実現する。

【0076】（受信端末側で生成される情報）次に総合データ配信サービスにおいて受信端末内で生成される各情報の生成時の処理について説明する。

【0077】（プロフィール生成）図44に、プロフィールの生成処理の説明図を示す。まず事前契約用メタデータより生成されるプロフィールについて図44を用いて説明する。プロフィール310とは、事前契約用メタデータ262を元にRMP内部で生成される情報である。プロフィール310の生成は、まず、送出側より受信した事前契約用メタデータ263をメタデータ復号機能により復号したのち、RMPコントローラ306により、事前契約用メタデータ263のユーザー識別情報275内の端末ID、個人IDにより端末全体用の契約情報か、各ユーザー用の契約情報かを判定し、メタデータ復号機能により復号された個人情報277、契約情報278より必要な情報のみを抽出し個人契約情報274を生成する。さらに、その個人契約情報274を、ユーザー識別情報275により識別したセキュリティエリア317内の全体プロフィール315、個人プロフィール316の各プロフィールに格納することにより、プロフィール310が生成される。

【0078】（鍵管理テーブル）図45に、鍵管理テーブルの生成処理の説明図を示す。次に鍵管理テーブルの生成時の処理について図45を用いて説明する。鍵管理テーブル311には、ユーザーの受信端末購入時に予め格納されているID、鍵情報と、ユーザーがサービス受信時に生成されるID、鍵情報が存在する。予め格納されている情報としては、端末ID249、端末鍵Kmc43、システムID247、システム鍵Ksy264が存在する。なお、システム鍵Ksyは、システム鍵Ksy1～Ksy3等のシステム鍵の総称である。この例では、システムID、鍵については、運用に使用されるID、鍵情報Ksy1と、システム鍵更新時に利用される予備用のID、鍵情報Ksy2の2種類が存在する。受信側で生成もしくは更新される部分としては、システム鍵更新時のシステムID247、システム鍵Ksy264、事業者ID248、事業者鍵Kw44、コンテンツID246、コンテンツ鍵Kk33が該当する。生成される各ID、鍵情報は、受信端末が受信したシステム鍵更新用メタデータ289、事前契約用メタデータ263、鍵配信用メタデータ256内の暗号化部分に格納されているため、RMP16内部のメタデータ復号により復号後に、RMPコントローラにより各メタデータから抽出

され、セキュリティの守られた記憶エリア317に格納することにより鍵管理テーブル311を生成する。

【0079】(検索/EPGテーブル)図46に、検索/EPGテーブルの生成処理の説明図を示す。検索/EPGテーブルについて図46を用いて説明する。検索/EPGテーブル312とは、受信したEPG用メタデータ254、蓄積/再生用メタデータ255よりRMP内部にコピーを作成し、メタデータ復号機能により各メタデータを復号後に、RMPコントローラにより必要項目を抽出し、蓄積媒体4内の所定位置に格納することにより生成される。検索/EPGテーブル312は、蓄積媒体内に複数存在するEPG用メタデータ254、蓄積/再生用メタデータ255の簡易情報の集合である。また、検索/EPGテーブル312は、暗号化せずに蓄積媒体に格納される情報であるため、受信端末上の検索アプリケーション、EPGアプリケーションから直接アクセス可能となり、受信端末の検索スピード、EPG表示スピードの向上が可能となる。

【0080】(予約情報)図47に、予約情報の生成処理の説明図を示す。次に予約情報について図47を用いて説明する。予約情報313とは、ユーザーの視聴/蓄積要求に対しRMP16内部でEPG用メタデータ254、プロファイル310より生成される情報であり、暗号化せずに蓄積媒体4に格納される情報である。ユーザーより視聴/蓄積要求が起こると、RMPコントローラ306は、視聴要求の対象となるコンテンツに対するEPG用メタデータ254のコピーをRMP内部に生成し、コピーしたEPG用メタデータをメタデータ復号機能により復号する。そして、RMPコントローラ306は、復号したEPG用メタデータの利用制限情報と、プロファイル内の予約要求を行ったユーザーの個人契約情報とにより、コンテンツ自体の予約が可能か、ユーザーの契約形態が要求コンテンツの予約が可能かを判定し、その後蓄積媒体4内の他の予約情報313により登録済みの予約がないか、スケジュール的に予約が可能かを判定する。ここで、RMPコントローラ306は、予約が可能であれば個人契約情報より予約を行ったユーザーの個人ID、EPG用メタデータ254より、コンテンツID、コンテンツサイズ、放送予定日時等、ユーザーの要求より予約の種別を抽出し予約情報313を生成し、蓄積媒体4内の所定位置に格納することで予約を行う。ユーザーの嗜好性を利用した自動蓄積を行わせる場合も同様に予約情報を生成する。

【0081】(ICカード内の個人契約情報)図48に、個人契約情報の生成処理の説明図を示す。次にプロファイル内の個人契約情報をICカードに格納する際の暗号化処理について図48を用いて説明する。ICカード15内の個人契約情報とは、基本的にRMP16内のセキュリティの守られた記憶エリア上のプロファイル内に格納されている個人契約情報274を暗号化させたものである。RMPコントローラ306は、ICカード15が挿入されたことを認識するとICカード15内のセキュリティエリア

上の個人ID270をセキュリティの守られた伝送路を通じて読み取り、プロファイル内の該当個人契約情報を識別する。次に、RMPコントローラ306は、ICカード15内に個人契約情報が存在すれば、それを読み取りメタデータ復号機能によりそれを復号し、互いの個人契約情報の非暗号化部分に格納されるバージョンNo.を確認し、ICカードのバージョンが新しい場合は、ICカード側の暗号化された個人契約情報をRMP内にコピーし、ICカード15よりセキュリティの守られた伝送路を通じて取得した個人鍵Km265を使用しメタデータ復号により個人契約情報を復号し該当するプロファイル内の個人契約情報を更新する。RMPコントローラ306は、逆にプロファイル側の個人契約情報274のバージョンが新しい場合は、ICカード15よりセキュリティの守られた伝送路を通じて取得した個人鍵Km265を使用し、メタデータ暗号機能309により個人契約情報の必要部分を暗号化したのちICカード15内の所定の位置に格納することにより個人契約情報の更新を行う。

【0082】(許諾情報)図49に、許諾情報の生成処理の説明図を示す。次に許諾情報について図49を用いて説明する。許諾情報314とは、コンテンツの視聴に対しての権利情報であり、RMP16内でICカード15内の個人契約情報274と、蓄積媒体4内の蓄積/再生用メタデータ255のコピーより生成される。ユーザーのコンテンツに対する視聴要求が起こると、RMPコントローラ306は該当するコンテンツに対する蓄積/再生用メタデータ255のコピーをRMP16内部に生成し、コピーした蓄積/再生用メタデータ255をメタデータ復号機能により復号する。蓄積/再生用メタデータを復号化した後、RMPコントローラ306は、ICカード15内より暗号化された個人契約情報274及び、セキュリティの守られた伝送路を通じて個人鍵Km265を取得し、メタデータ復号により個人契約情報274を復号する。個人契約情報を復号化した後、RMPコントローラ306は、蓄積/再生用メタデータ255内の利用制限情報と、個人契約情報によりユーザーが視聴可能なコンテンツかを判定し、ユーザーの選択する視聴契約形態により、蓄積/再生用メタデータ内の契約情報、課金情報等より必要な項目を抽出し許諾情報314を生成し、ICカード15より取得した個人鍵Km265を使用しメタデータ暗号機能309により暗号化したのちICカード内の所定位置に暗号化された許諾情報を格納する。また受信端末内でユーザーの嗜好性による自動蓄積予約、画面表示の変化などの処理を行わせる場合は、許諾情報内のジャンル等の情報を集計することによりユーザーの嗜好性を判断することで、処理が可能となる。以上が総合データ配信サービスにおける受信端末内で生成される情報に対する処理である。総合データ配信サービスは、前述の送出側より配信される各メタデータ、受信側である受信端末内で配信されたメタデータを利用し各情報を生成、使用する

ことによりコンテンツの著作権、その他放送事業者、ユーザー等の権利保護を可能とする。

#### 【0083】

【発明の効果】本発明によると、以上のように、蓄積型放送かつ、コンテンツの保護が可能となる制御情報を付加するデータ配信サービス方法を提供することができる。

#### 【図面の簡単な説明】

【図1】総合データ配信サービスの受信側の構成図。

【図2】総合データ配信サービスの全体システム構成図。

【図3】総合データ配信サービスにおける権利保護方式の説明図。

【図4】総合データ配信サービスと既存サービスの暗号化方式比較の説明図。

【図5】コンテンツの暗号化方式の説明図。

【図6】メタデータの暗号化方式の説明図。

【図7】総合データ配信サービスにおける限定受信方式の説明図。

【図8】事前契約による課金方式の説明図。

【図9】上り回線を必要としない視聴契約に対する課金方式の説明図。

【図10】上り回線を使用したオンライン課金方式の説明図。

【図11】総合データ配信サービスにおけるサービスの流れの説明図。

【図12】事前契約におけるサービスフローの説明図。

【図13】送出側におけるサービスフローの説明図。

【図14】受信側におけるサービスフローの説明図。

【図15】送出側システム全体の構成図。

【図16】配信センタ内の構成図。

【図17】オーサリングシステム内の構成図。

【図18】番組構成管理システム内の構成図。

【図19】PSI/SI生成装置の説明図。

【図20】メタデータ生成装置の説明図。

【図21】コンテンツ暗号化装置の説明図。

【図22】メタデータ暗号化装置の説明図。

【図23】送出系システム内の構成図。

【図24】鍵管理センタ内の構成図。

【図25】鍵生成装置の説明図。

【図26】鍵管理サーバの説明図。

【図27】顧客管理センタ内の構成図。

【図28】顧客情報生成システム内の構成図。

【図29】顧客情報管理システム内の構成図。

【図30】事前契約用メタデータの構成および格納される情報の説明図。

【図31】EPG用メタデータの構成および格納される情報の説明図。

【図32】蓄積/再生用メタデータの構成および格納される情報の説明図。

【図33】鍵配信用メタデータの構成および格納される情報の説明図。

【図34】メタデータリストの構成および格納される情報の説明図。

【図35】システム鍵更新用メタデータの構成および格納される情報の説明図。

【図36】受信端末内の構成図。

【図37】メタデータ復号機能の説明図。

【図38】コンテンツ復号機能の説明図。

【図39】プロフィールの構成図。

【図40】鍵管理テーブルの構成図。

【図41】メタデータ暗号機能の説明図。

【図42】蓄積媒体内に格納される情報の蓄積状態の説明図。

【図43】ICカード内の構成の説明図。

【図44】プロフィールの生成処理の説明図。

【図45】鍵管理テーブルの生成処理の説明図。

【図46】検索/EPGテーブルの生成処理の説明図。

【図47】予約情報の生成処理の説明図。

【図48】個人契約情報の生成処理の説明図。

【図49】許諾情報の生成処理の説明図。

【図50】映像系及びデータ系コンテンツを構成するデータの説明図。

【図51】本総合データ配信サービスにおいてコンテンツ、前述した各メタデータを暗号化する際に使用する暗号鍵、暗号鍵についての説明図。

【図52】RMPコントローラ306の行う主な制御処理の説明図。

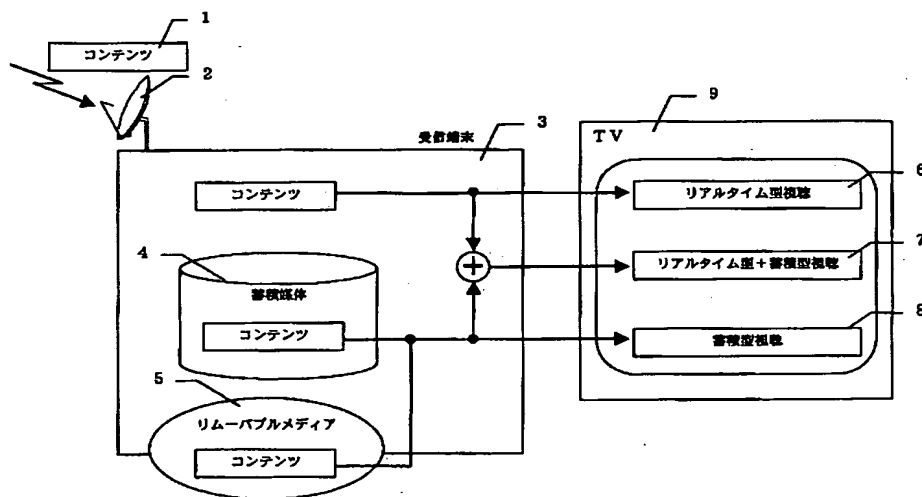
#### 【符号の説明】

- 30 1…コンテンツ、2…アンテナ、3…受信端末、4…蓄積媒体、5…リムーバブルメディア、6…リアルタイム型視聴、7…リアルタイム型+蓄積型視聴、8…蓄積型視聴、9…TV、10…衛星、11…地上回線、12…流通網、13…携帯電話網、14…外部機器、15…ICカード、16…RMP、17…暗号化コンテンツ、18…暗号化メタデータ、19…PSI/SI、20…コンテンツ生成、21…TSP化、22…ペイロード、23…コンテンツの一部、24…ペイロード部分の暗号化、25…コンテンツ暗号化、26…暗号化コンテンツの一部、27…
- 40 映像系コンテンツ、28…データ系コンテンツ、29…MPEG2-Video (PES)、30…MPEG2-AAC (PES)、31…暗号化MPEG2-Video (PES)、32…暗号化MPEG2-AAC (PES)、33…Kk1、34…Kk2、35…暗号化必要部分、36…暗号化データ容量、37…暗号化データ、38…非暗号化メタデータ、39…契約要求、40…事前契約用メタデータ、41…鍵配信用メタデータ、42…蓄積/再生用メタデータ、43…端末鍵Kmc、44…事業者鍵Kw、45…ユーザー毎に配信、46…コンテンツ要求、47…ユーザー登録、48…指定口座、49…ポイント
- 50 要求、50…課金情報、51…PPV登録、100…送出

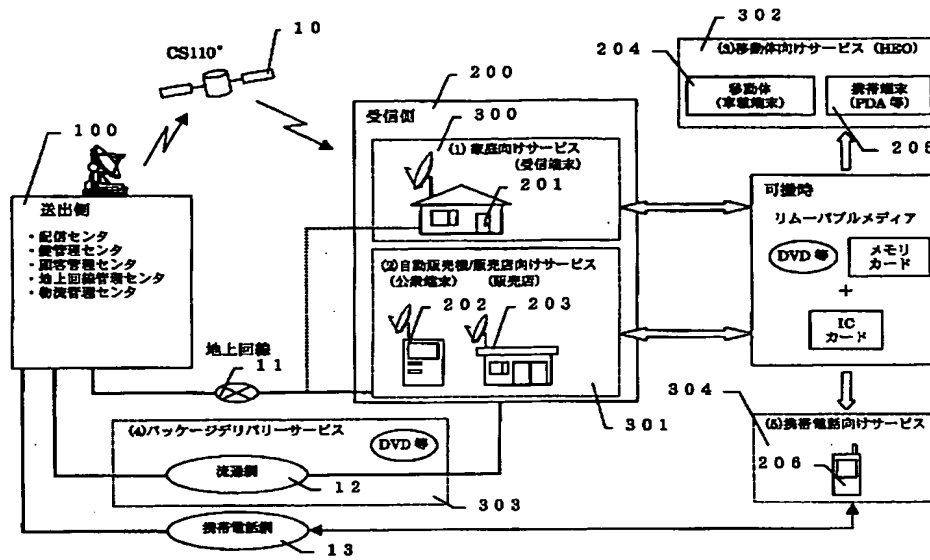
側、101…送出側フロー、102…コンテンツ生成、103…メタデータ生成、104…暗号化/配信、105…事前契約フロー、106…ユーザー、107…顧客管理、150…ユーザー情報、200…受信側、201…家庭、202…自動販売機、203…販売店、204…車載端末、205…携帯端末、206…携帯電話、208…番組編成、209…コンテンツ暗号化、210…PSI/SI生成、211…メタデータ暗号化、212…配信フォーマット化、213…物流管理センタ、214…地上回線管理センタ、220…配信センタ、221…オーサリングシステム、222…番組構成管理システム、223…メタデータ生成装置、224…PSI/SI生成装置、225…コンテンツ暗号化装置、226…メタデータ暗号化装置、227…送出系システム、228…映像オーサリングシステム、229…音声オーサリングツール、230…データオーサリングツール、231…コンテンツ構成装置、232…コンテンツ管理サーバ、233…関連ファイル、234…素材、235…番組構成装置、236…番組運行スケジュール生成装置、237…番組管理サーバ、238…運行スケジュール、239…カレンダー生成装置、240…鍵管理センタ、241…パッケージタイザ、242…MUX、243…受託放送設備、244…鍵生成装置、245…鍵管理サーバ、246…コンテンツID、247…システムID、248…事業者ID、249…端末ID、250…メタデータリスト、251…EPG用メタデータ、252…蓄積/再生用メタデータ、253…鍵配信メタデータ、254…暗号化EPG用メタデータ、255…暗号化蓄積/再生用メタデータ、256…暗号化鍵配信メタデータ、257…鍵配信メタデータ

ータ(無料)、258…鍵配信メタデータ(有料)、259…事前契約用メタデータ、260…顧客管理センタ、261…暗号化鍵配信メタデータ(無料)、262…暗号化鍵配信メタデータ(有料)、263…暗号化事前契約用メタデータ、264…システム鍵Ksy、265…個人鍵Km、266…顧客情報生成システム、267…顧客情報管理サーバ、268…ユーザーI/F、269…顧客情報生成装置、270…個人ID、271…顧客情報管理システム、272…ICカード生成装置、273…事前契約用メタデータ生成装置、274…個人契約情報、275…ユーザー識別情報、276…暗号化情報、277…個人情報、278…契約情報、279…メタデータ属性情報、280…番組情報、281…コンテンツ情報、282…利用制限情報、283…コンテンツ暗号化情報、284…契約情報、285…課金情報、286…コンテンツ鍵情報、287…メタデータリスト属性情報、288…リスト情報、289…システム鍵更新用メタデータ、290…システム鍵情報、300…家庭向けサービス、301…自動販売機/販売店向けサービス、302…移動体向けサービス、303…パッケージデリバリサービス、304…携帯電話向けサービス、306…RMPコントローラ、307…メタデータ復号、308…コンテンツ復号、309…メタデータ暗号、310…プロフィール、311…鍵管理テーブル、312…検索/EPGテーブル、313…予約情報、314…許諾情報、315…全体プロフィール、316…個人プロフィール、317…セキュアメモリ、318…通常メモリ、331…受信側フロー、332…予約、333…コンテンツ受信/蓄積、334…視聴契約、335…再生

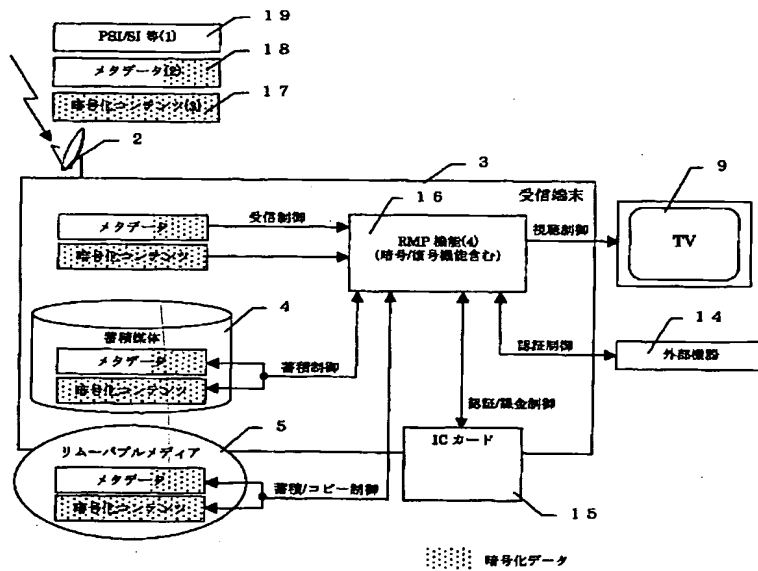
【図1】



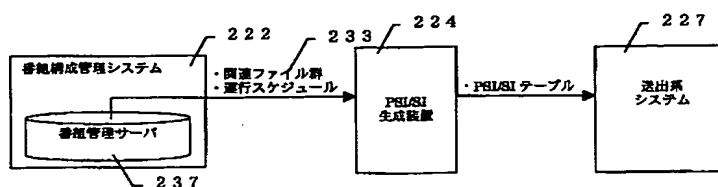
【図 2】



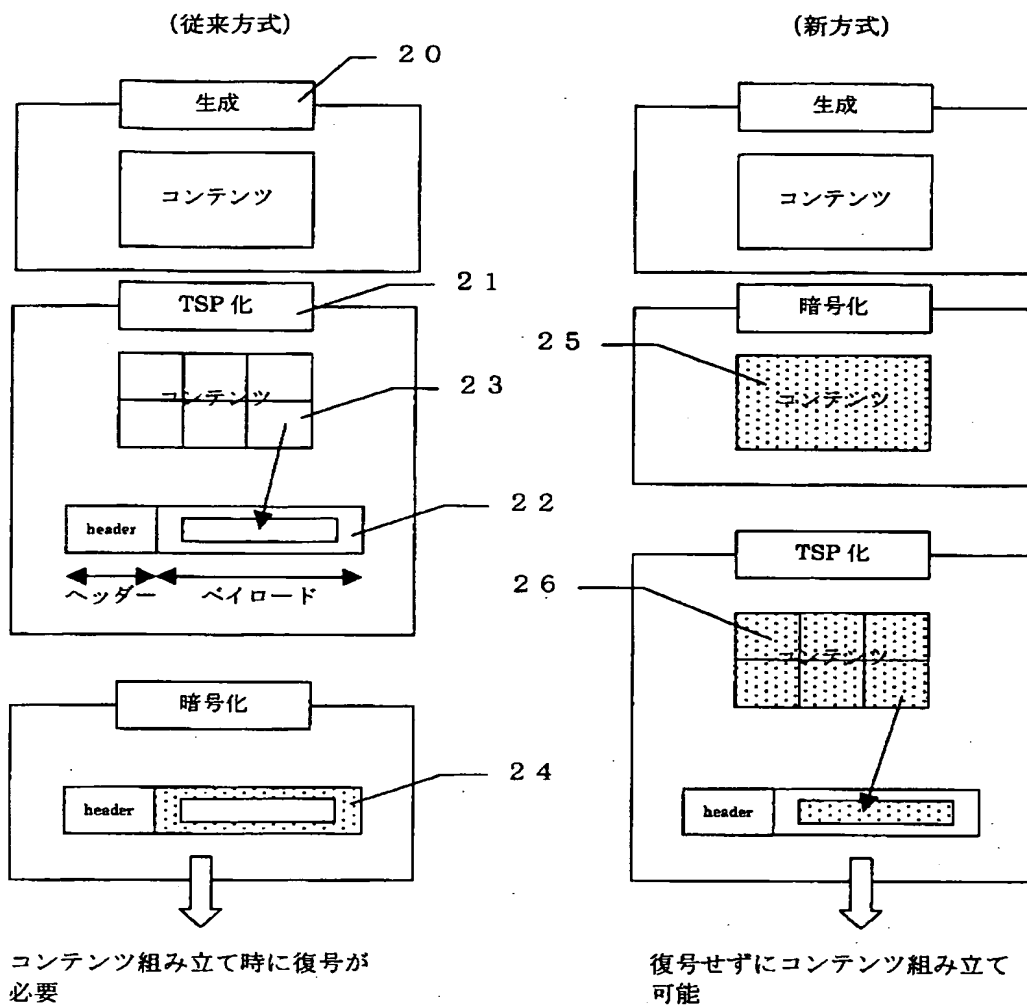
【図 3】



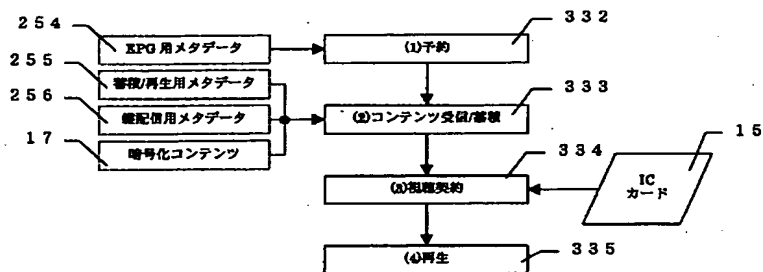
【図 19】



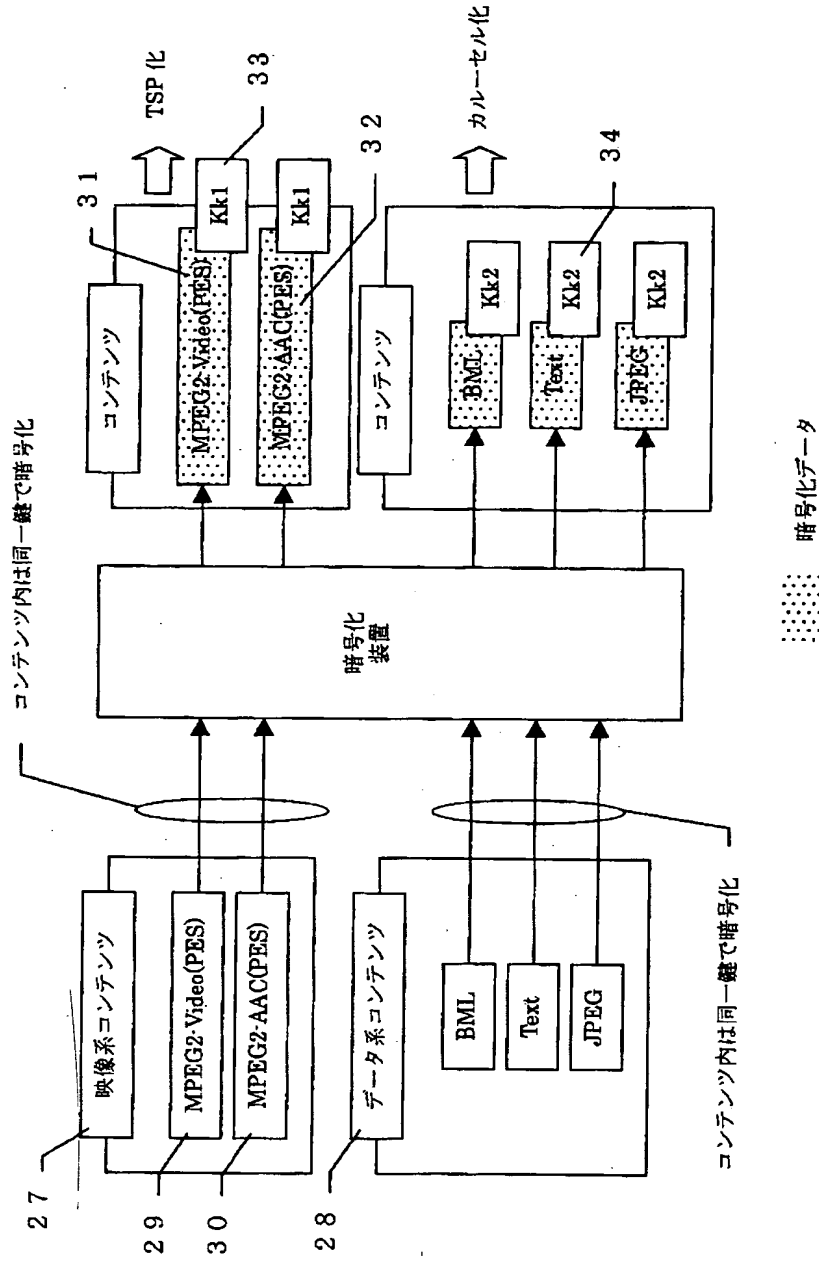
【図 4】



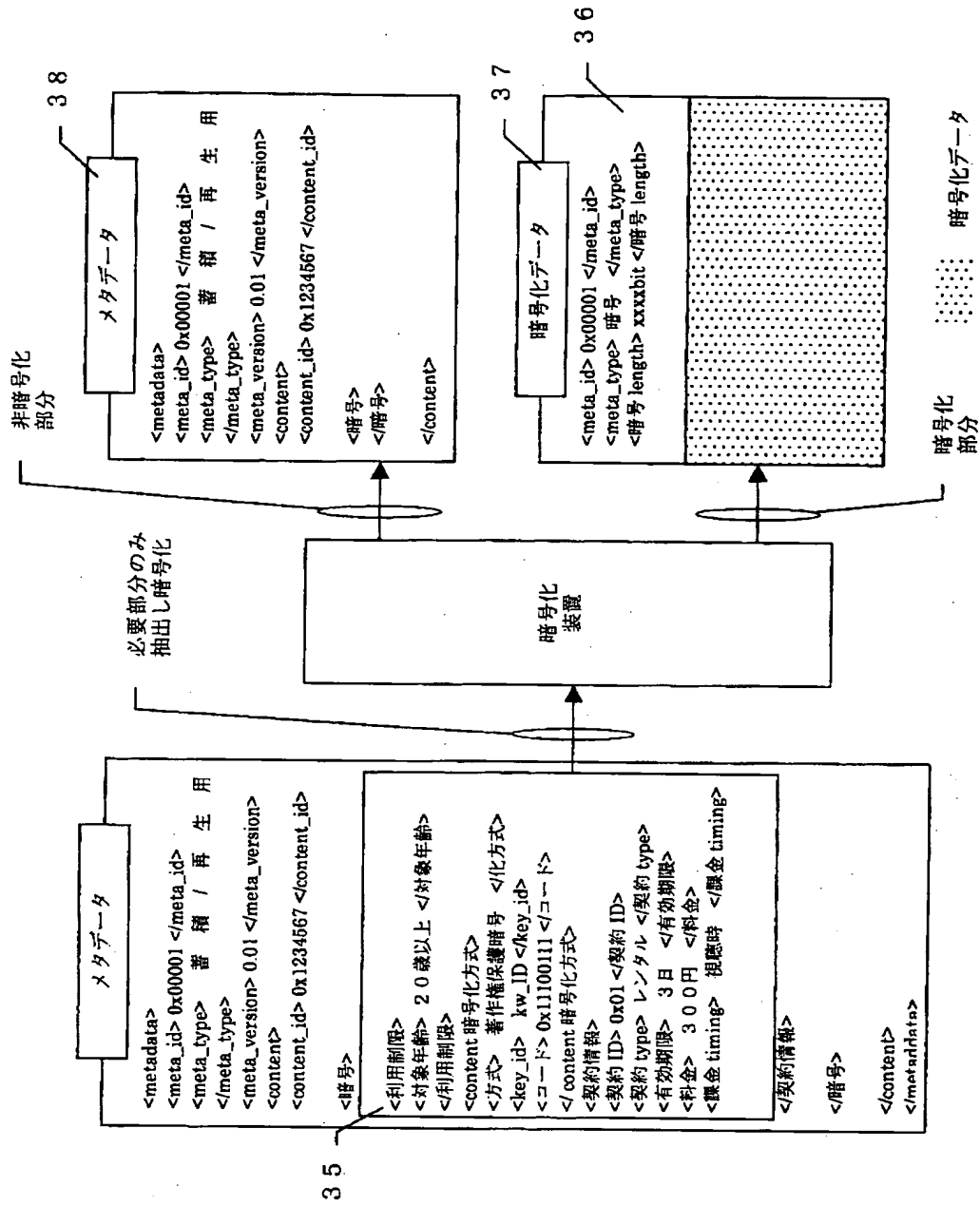
【図 14】



【図5】

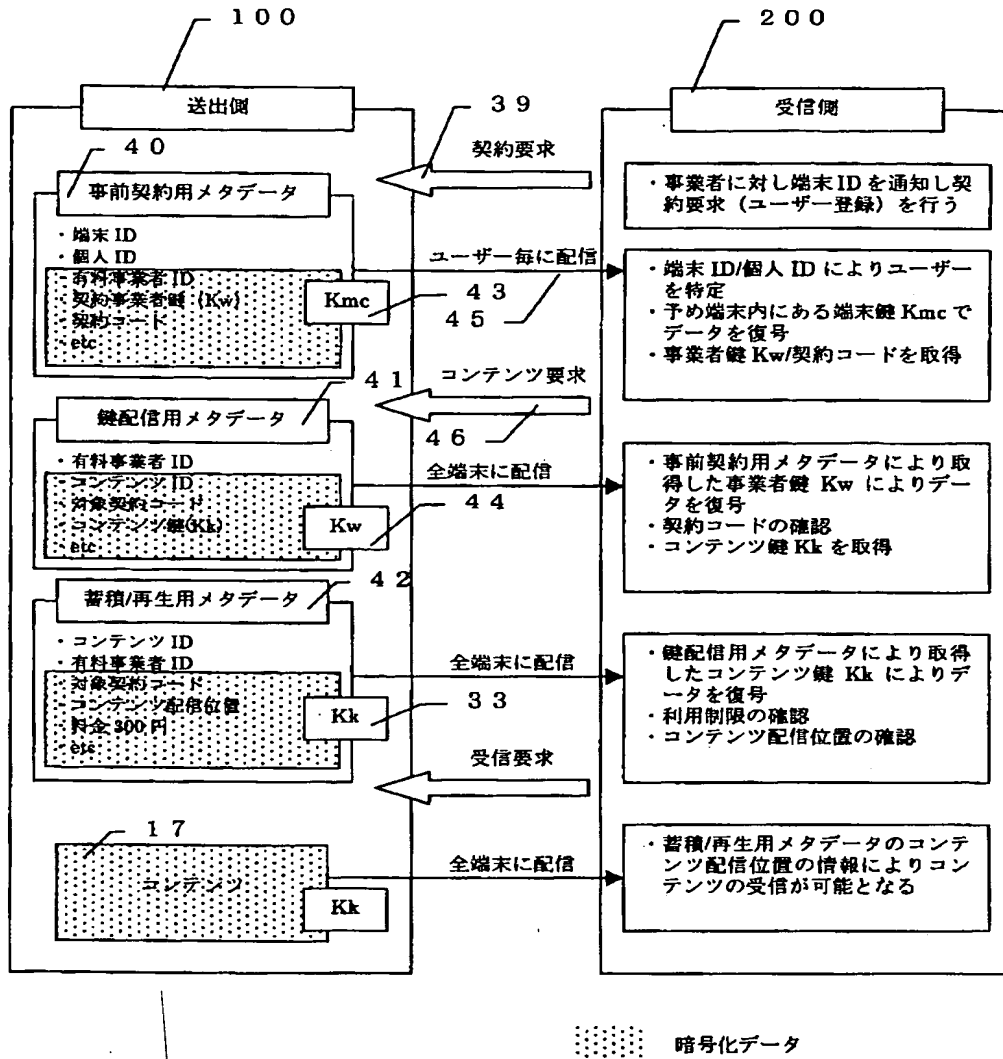


【図6】

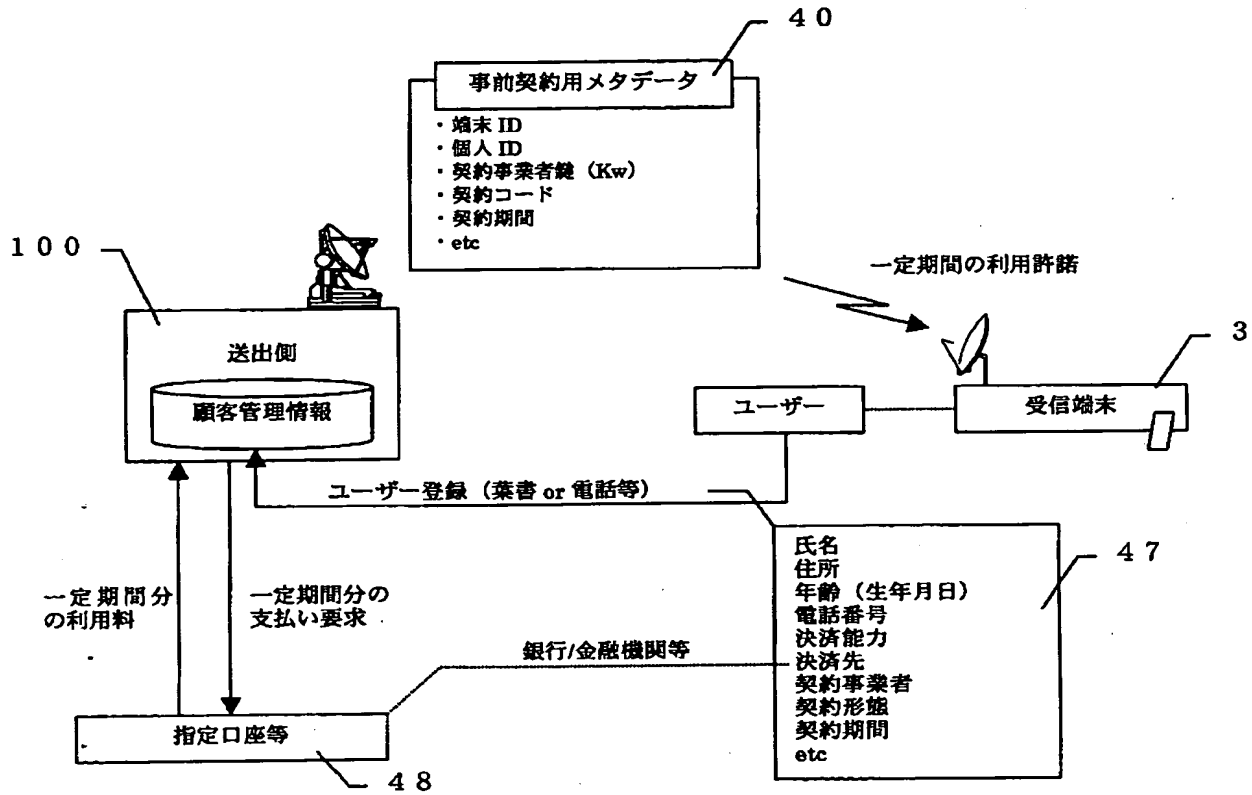




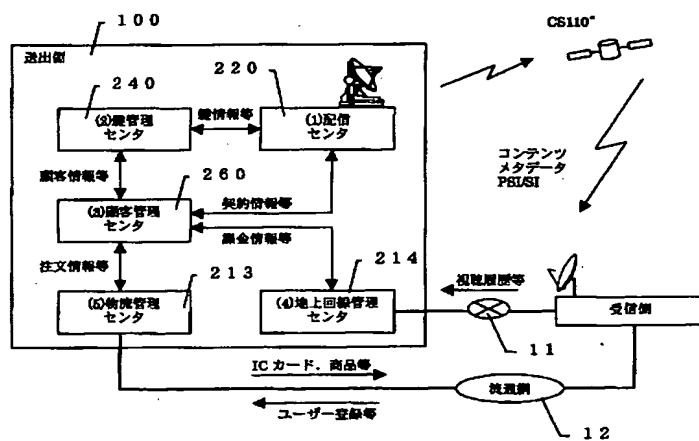
【図7】



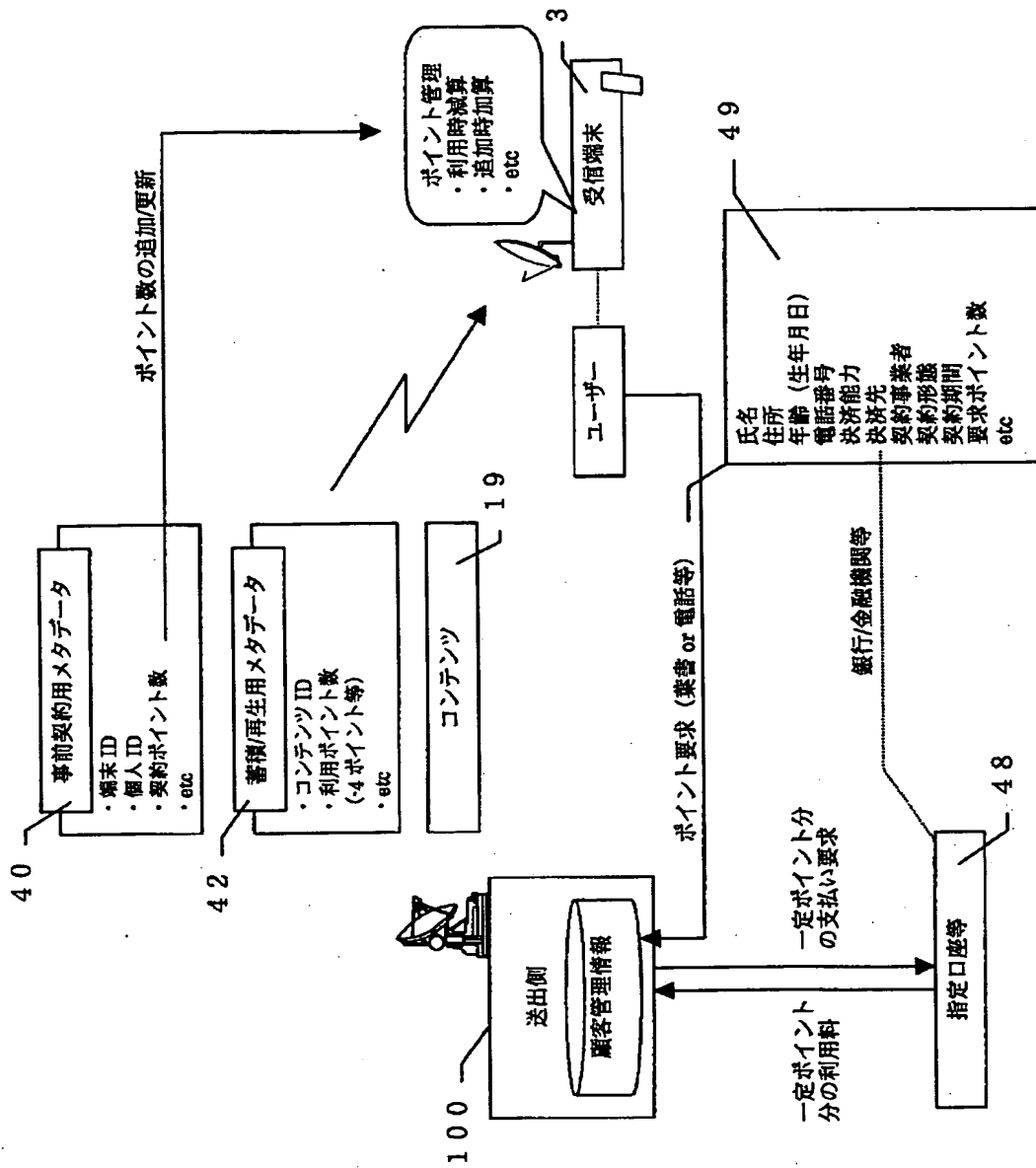
【図 8】



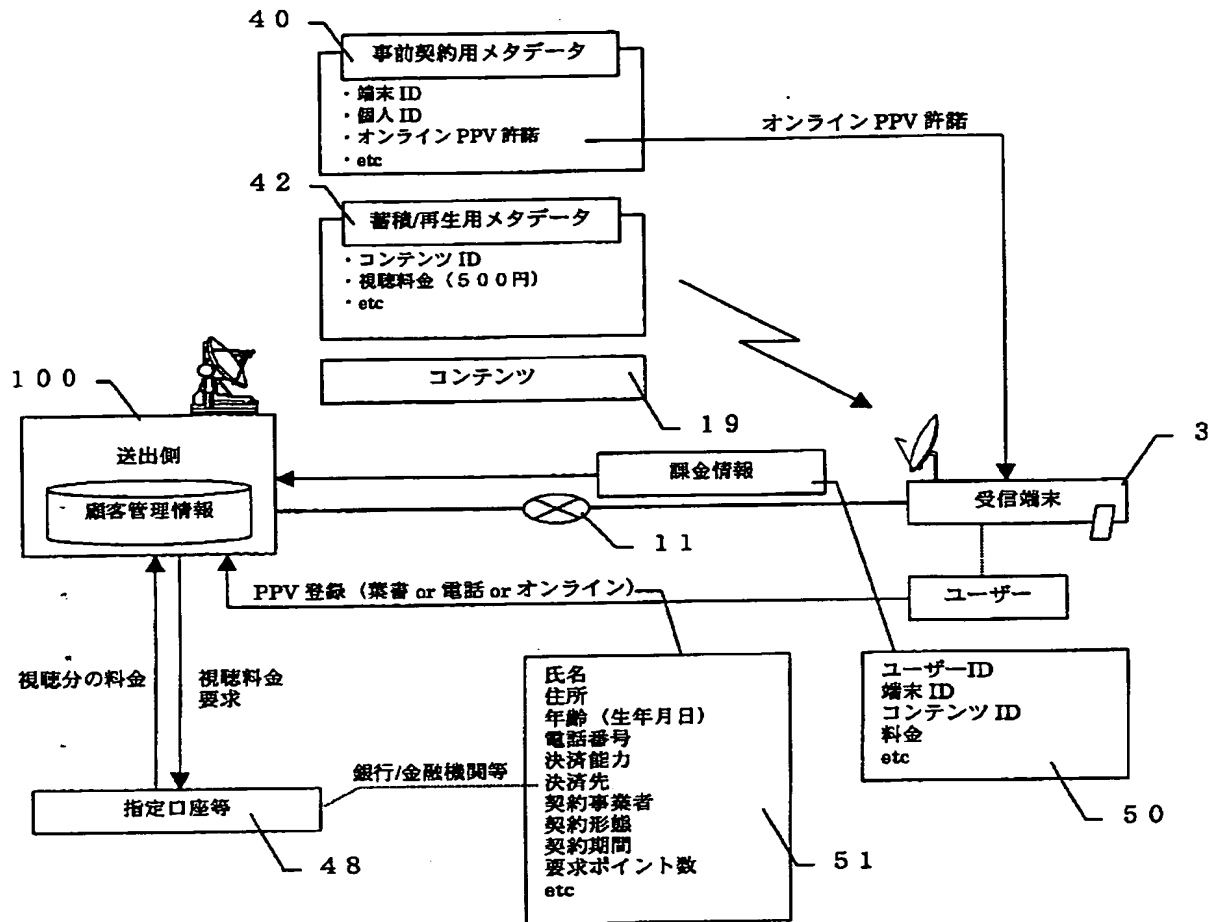
【図 15】



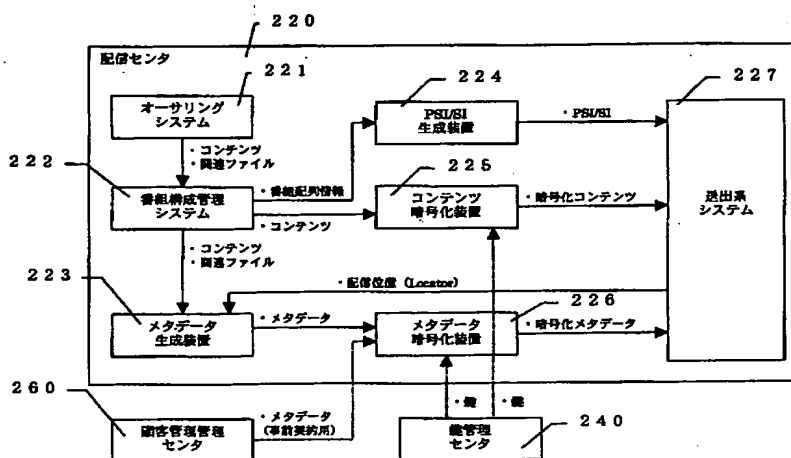
【图9】



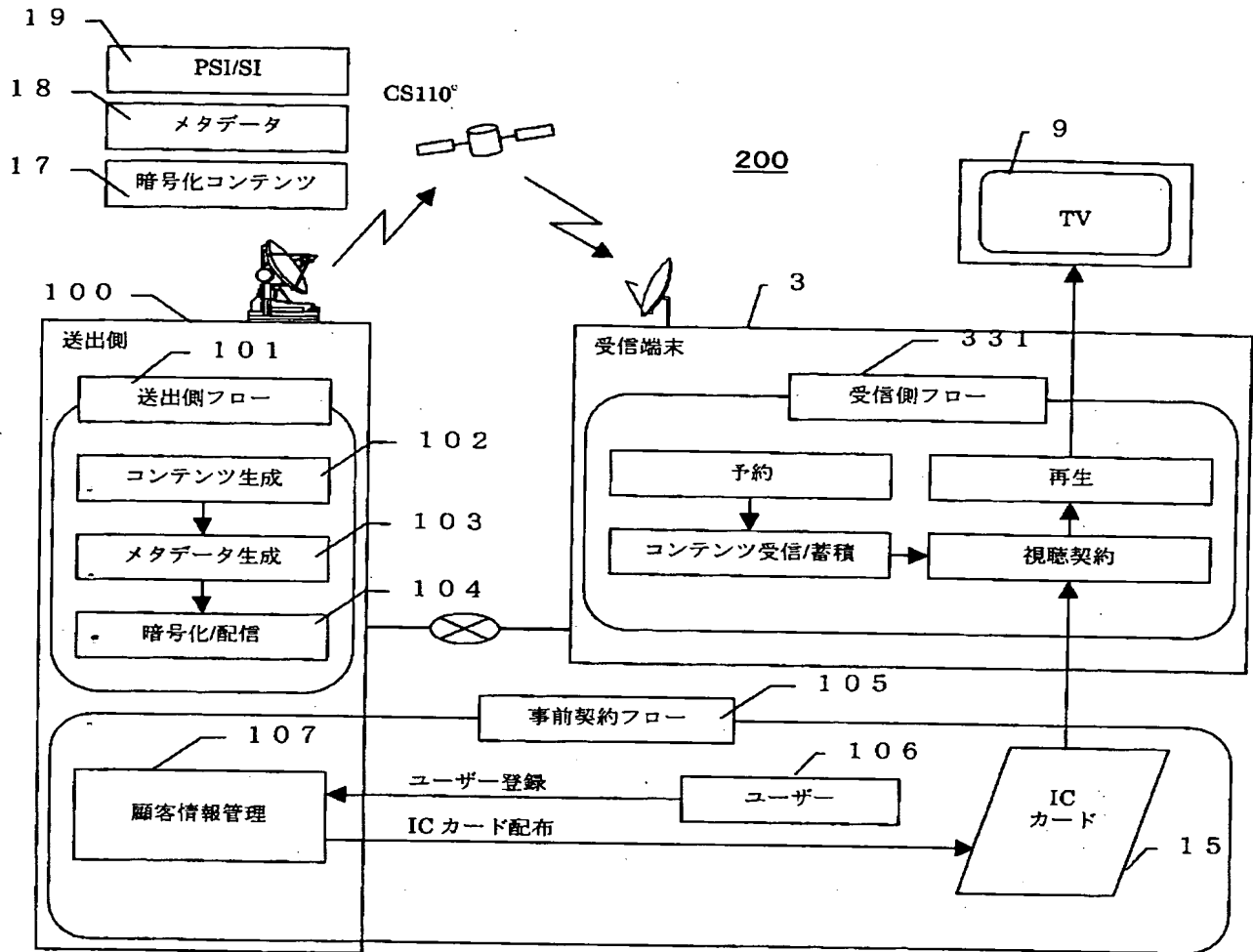
【図 10】



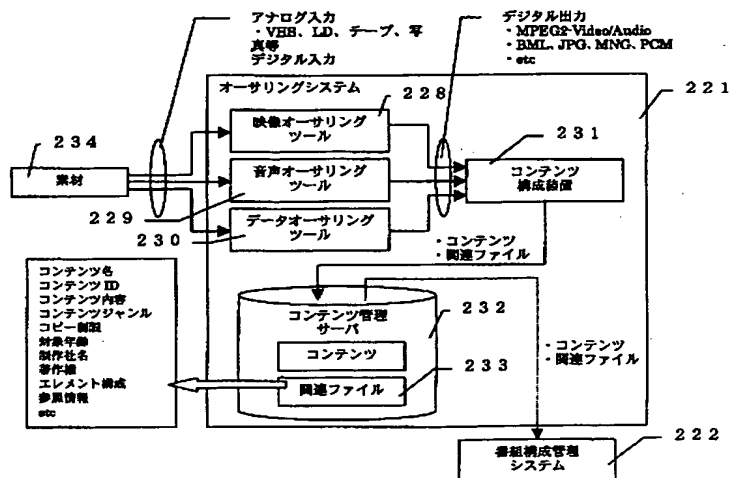
【図 16】



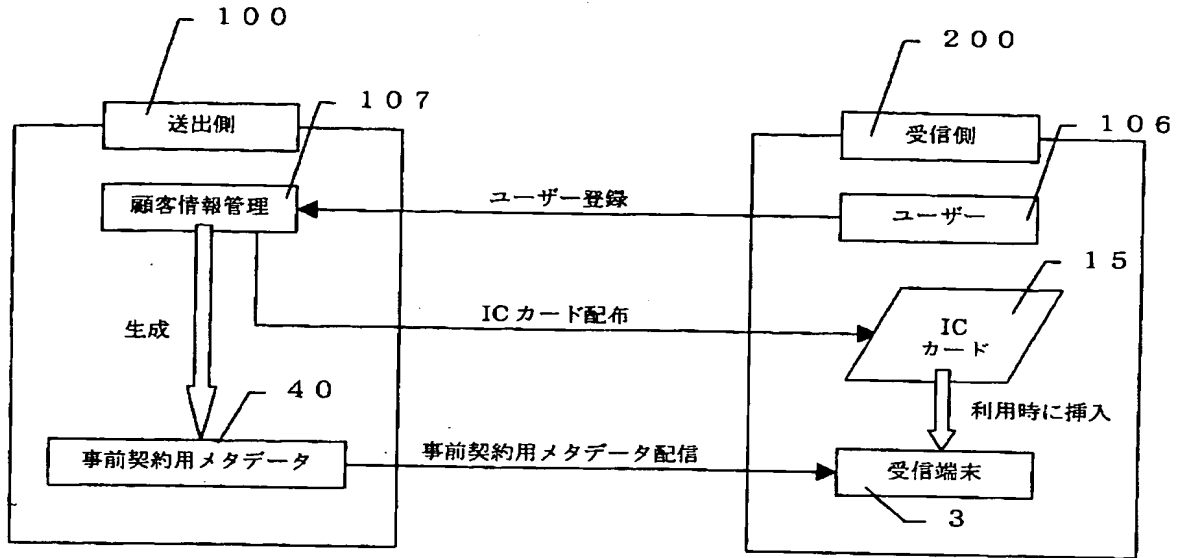
【図 11】



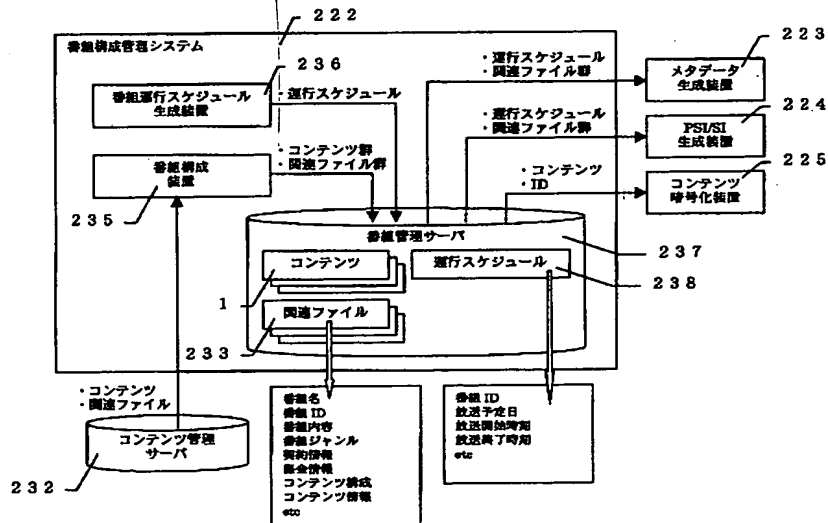
【図 17】



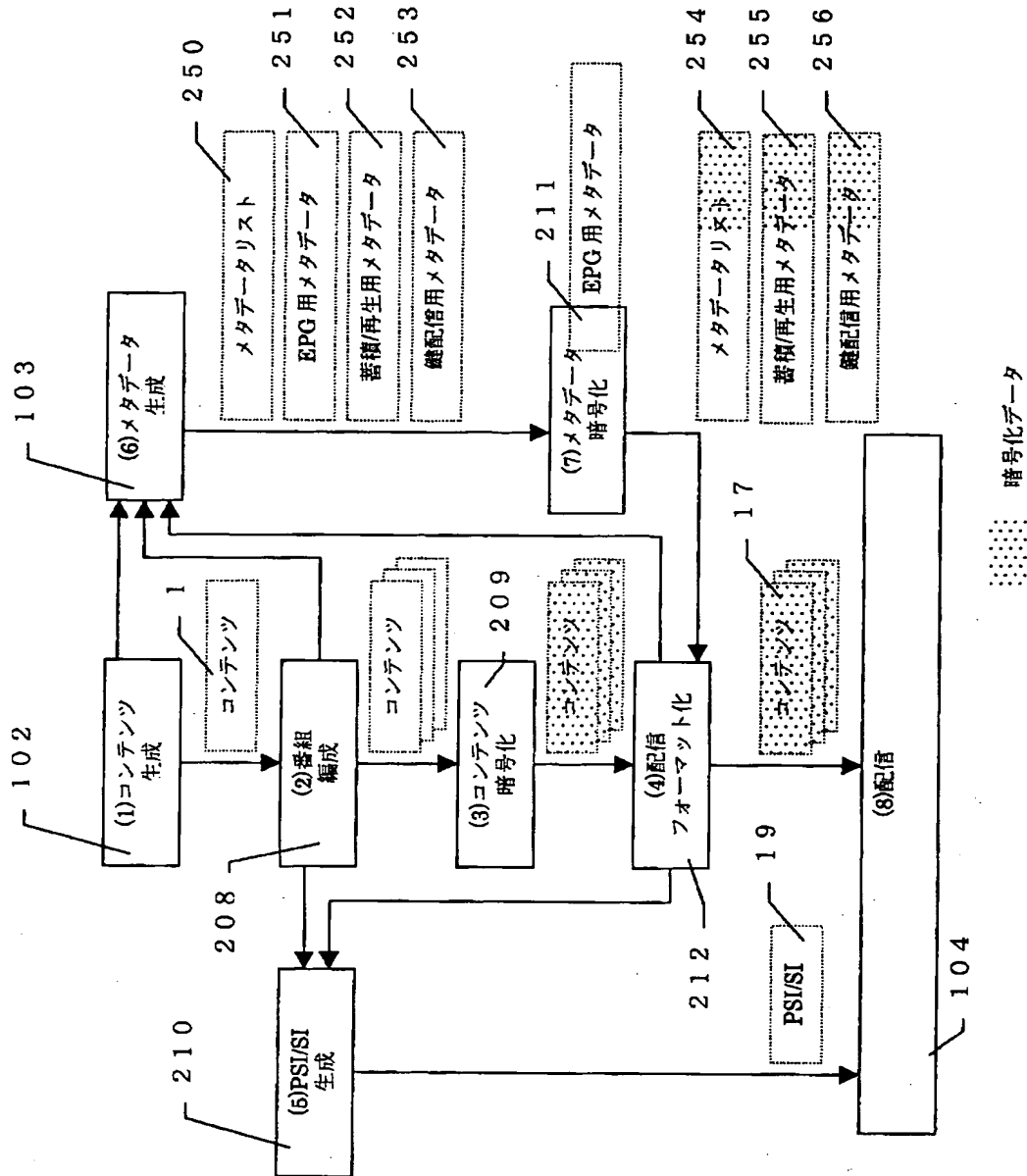
【図 12】



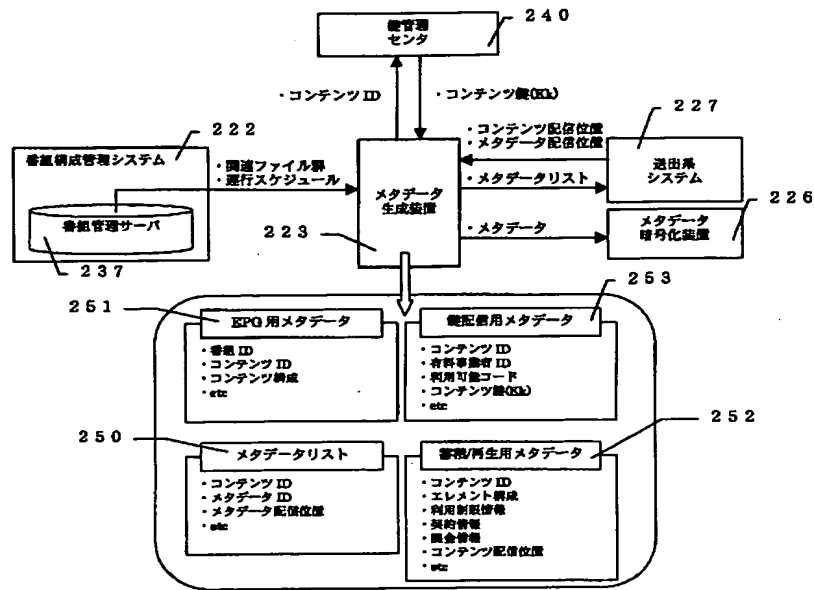
【図 18】



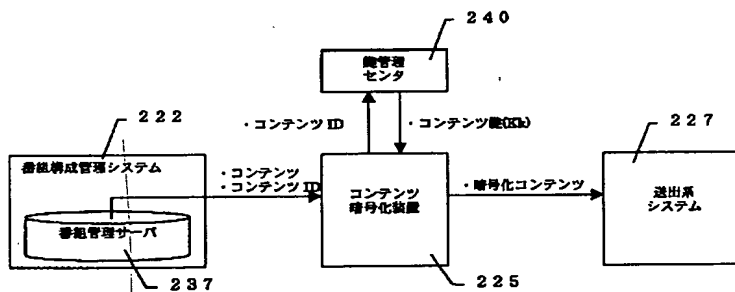
【図 13】



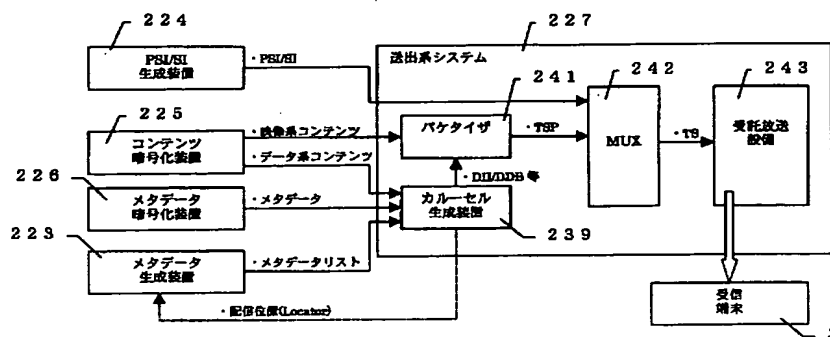
【図20】



【図21】

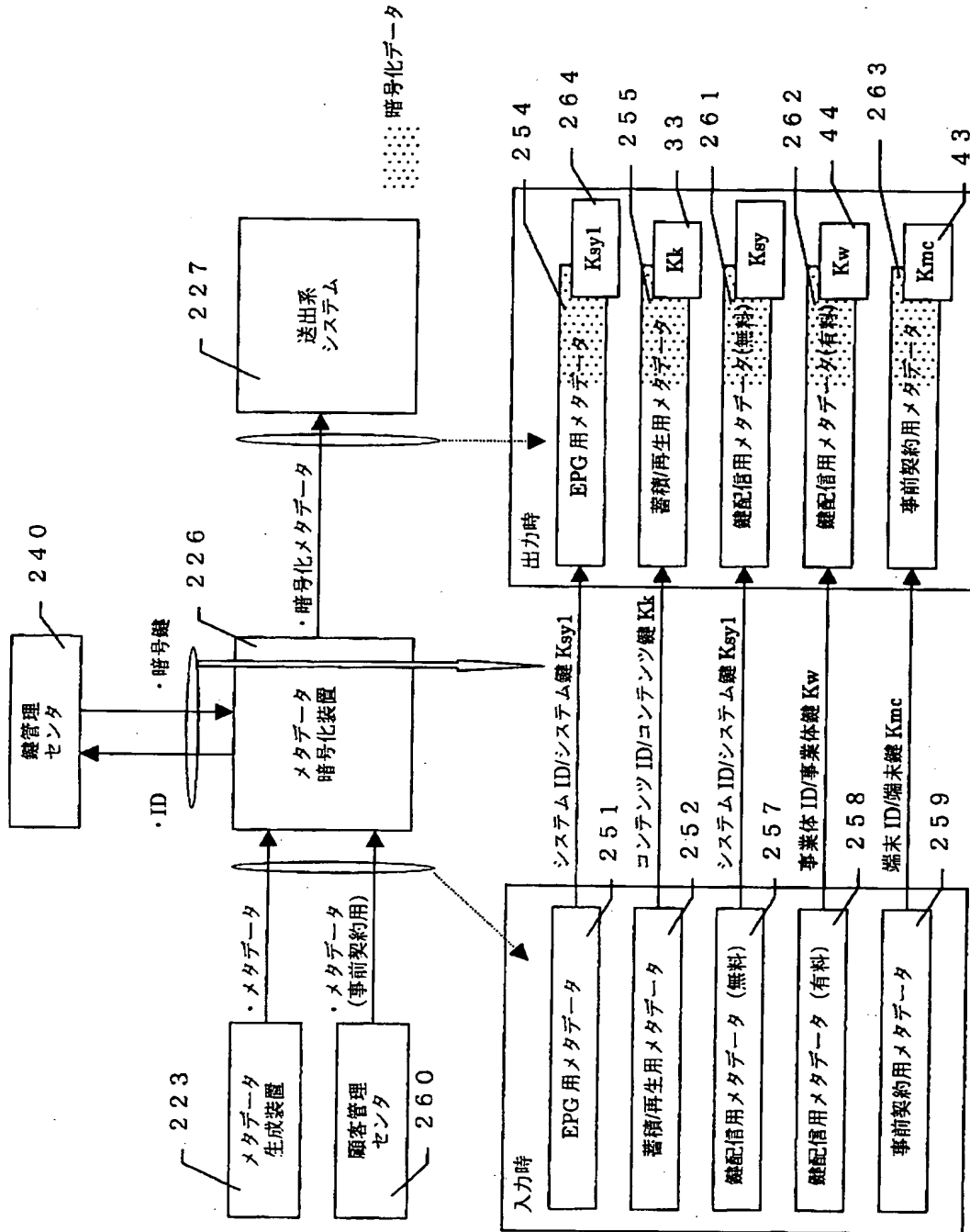


【図23】

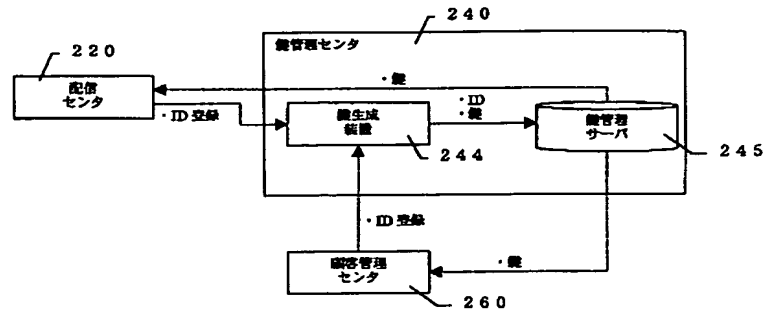




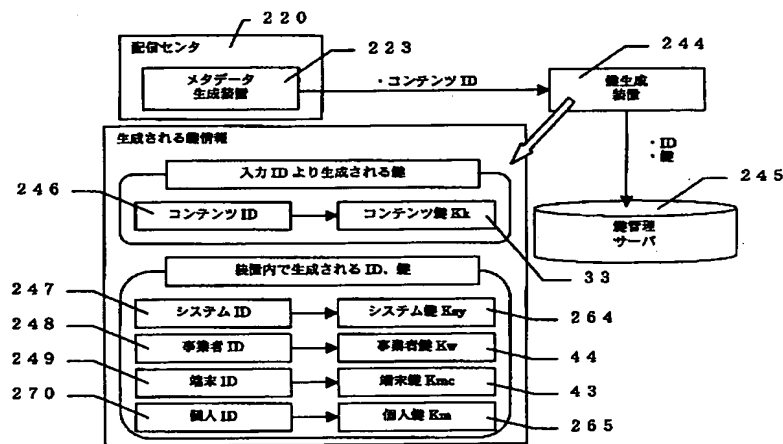
【図22】



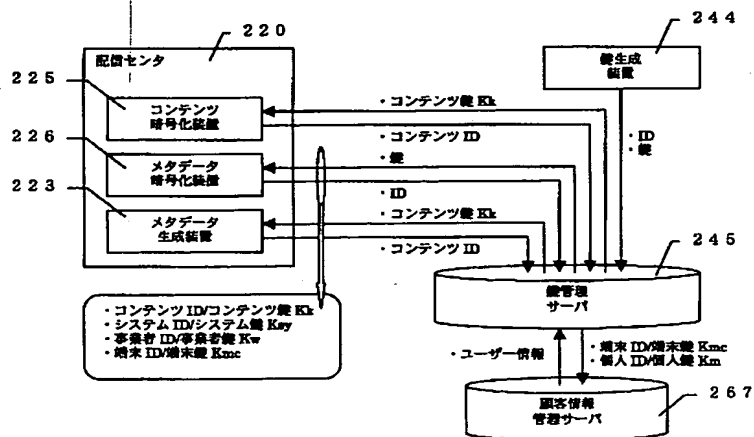
【図 24】



【図 25】



【図 26】



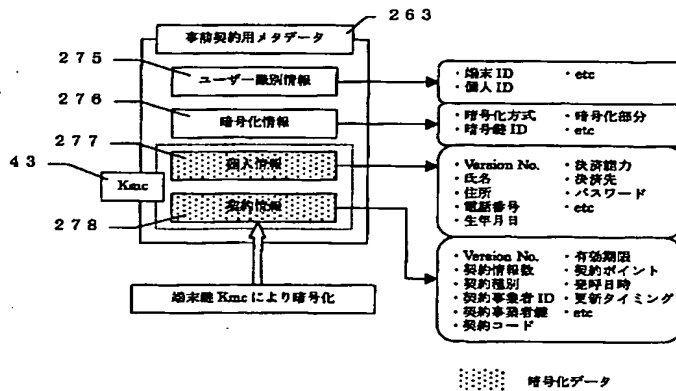
```

graph LR
    User[106 ユーザー] -- "・ユーザー登録" --> CGS[266 顧客情報生成システム]
    CGS -- "・顧客情報" --> MIS[271 顧客情報管理システム]
    MIS -- "・ICカード" --> User
    MIS <--> |"・ID, ・氏名"| MC[240 管理センター]
    MIS -- "・メタデータ (事前契約用), ・氏名" --> DC[220 配信センター]
    subgraph 260 [顧客管理センタ]
        CGS
        MIS
    end

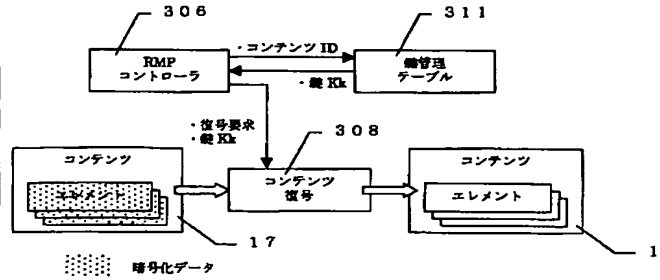
```

[illegible][illegible]

【図 30】

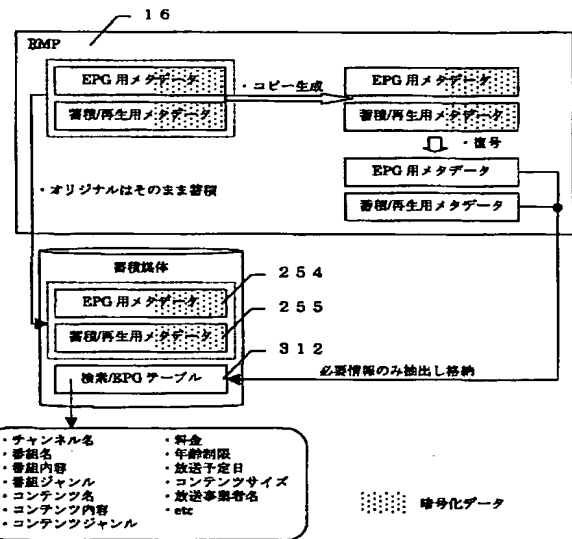
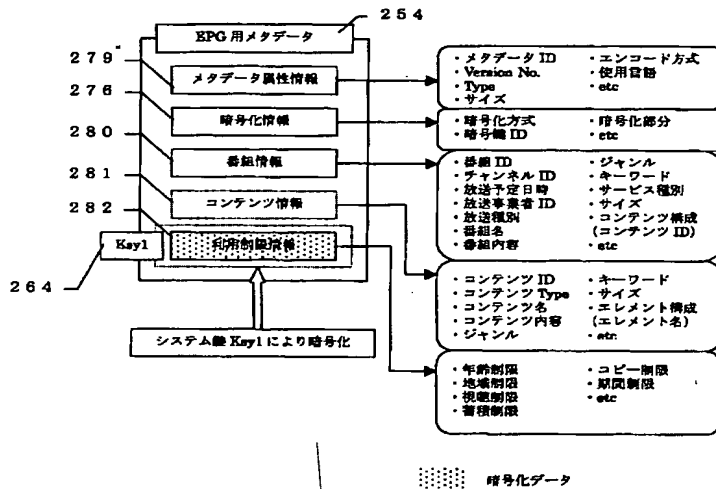


【図 38】

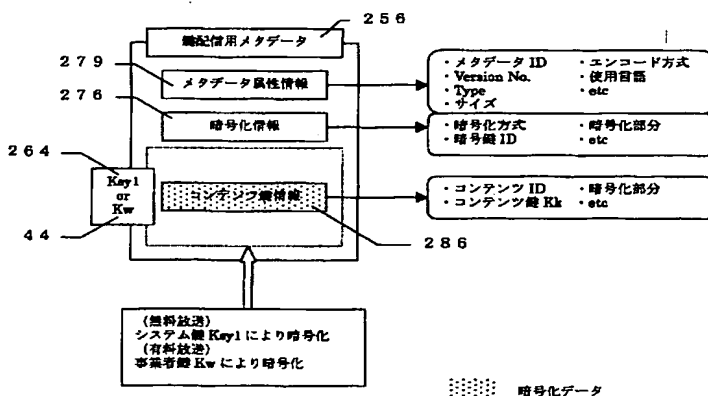


【図 46】

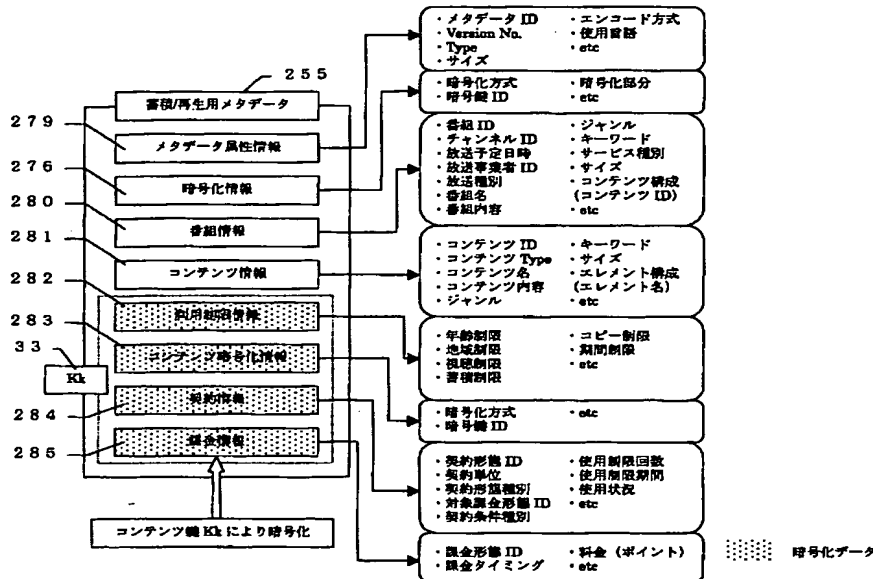
【図 31】



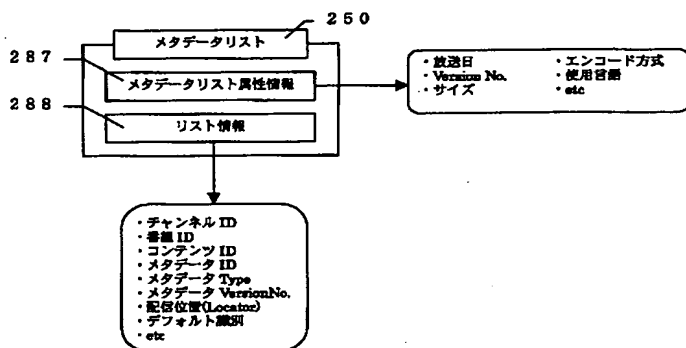
【図 33】



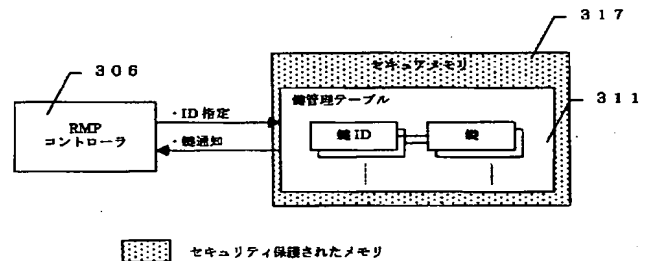
【図 32】



【図 34】

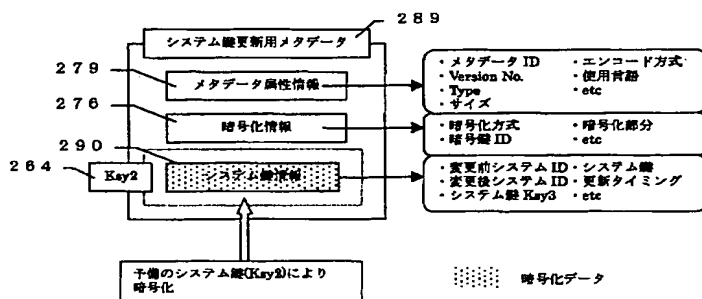


【図 40】



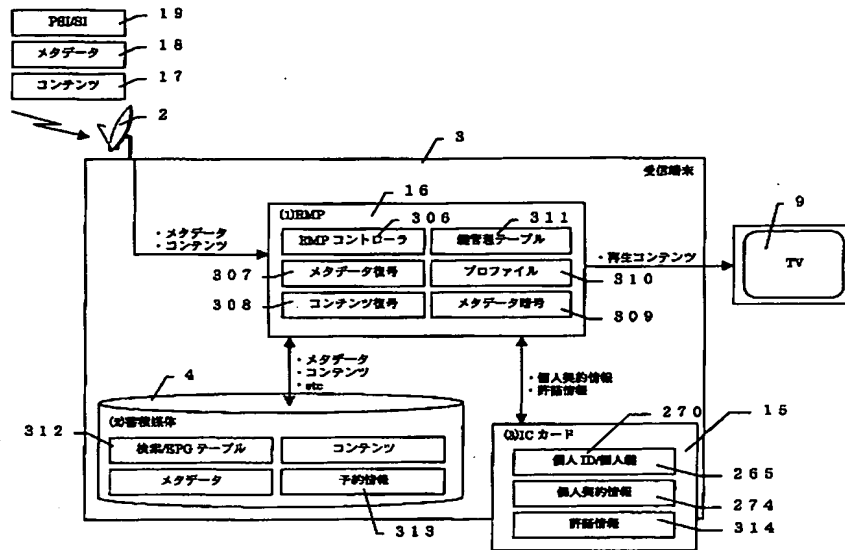
【図 50】

【図 35】

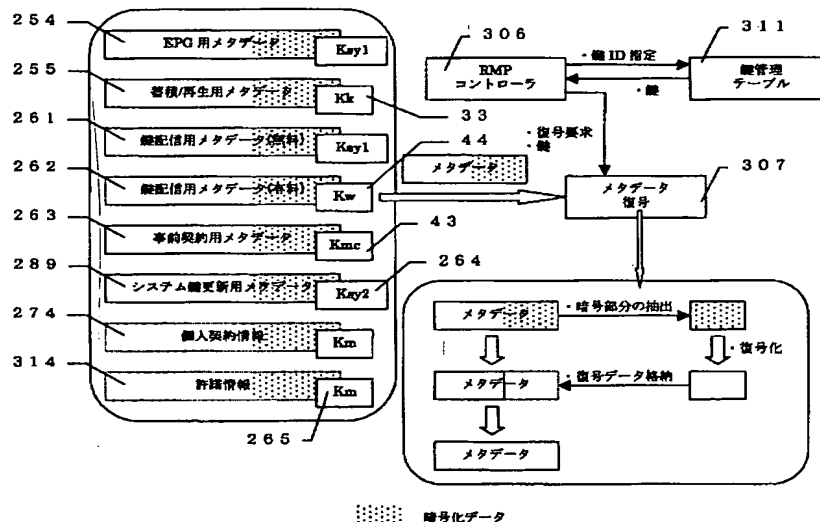


コンテンツ種別	エレメント
映像系コンテンツ	<ul style="list-style-type: none"> <li>MPEG2-Video stream (PES)</li> <li>MPEG2-Audio stream (PES)</li> <li>MPEG1-Video stream (PES)</li> <li>その他</li> </ul>
データ系コンテンツ	<ul style="list-style-type: none"> <li>XML</li> <li>Text</li> <li>JPG</li> <li>MNG</li> <li>MPEG2-Video</li> <li>MPEG2-Audio</li> <li>MPEG1-Video</li> <li>MPEG1-PES</li> <li>MPEG1-PES</li> <li>その他</li> </ul>

【图 3 6】

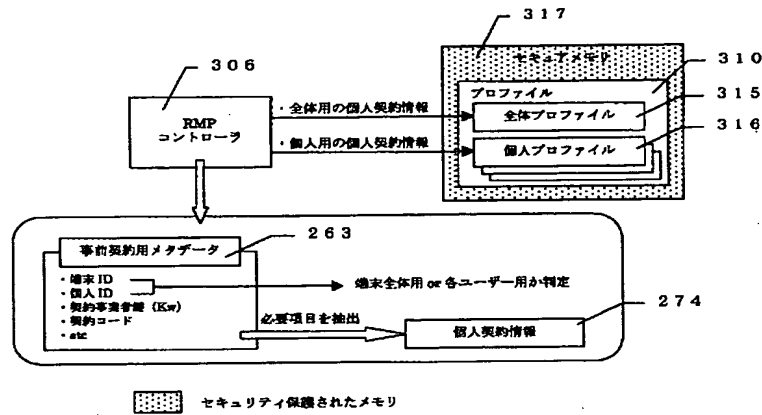


【図 3 7】

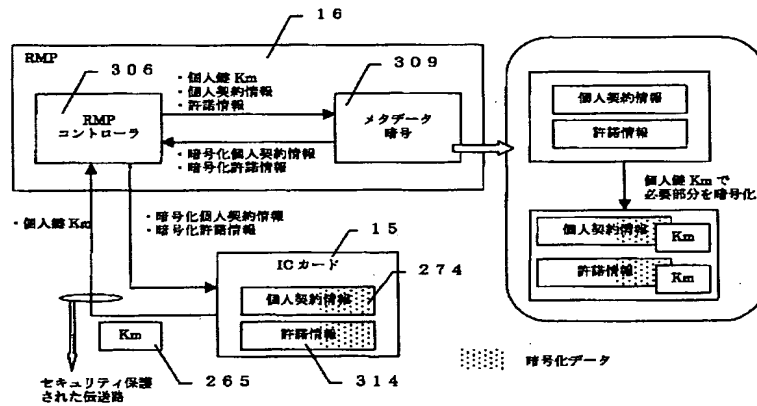


データ化番号

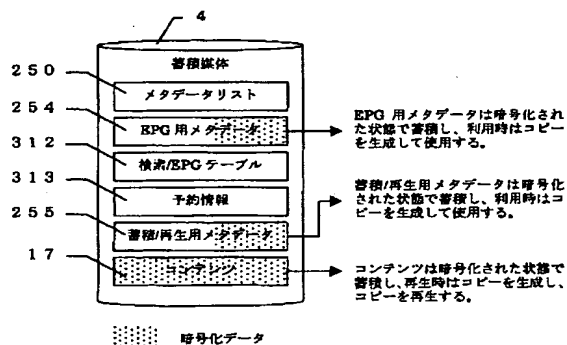
【図 39】



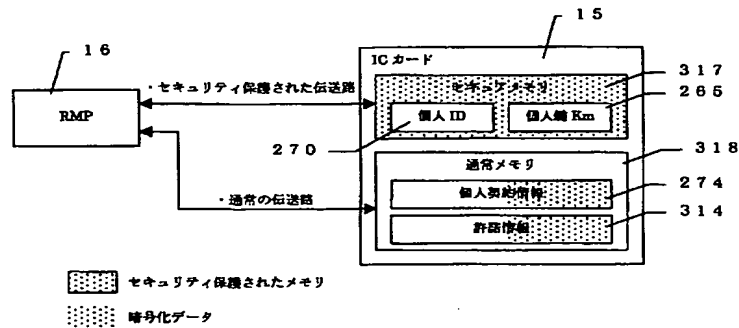
【図 41】



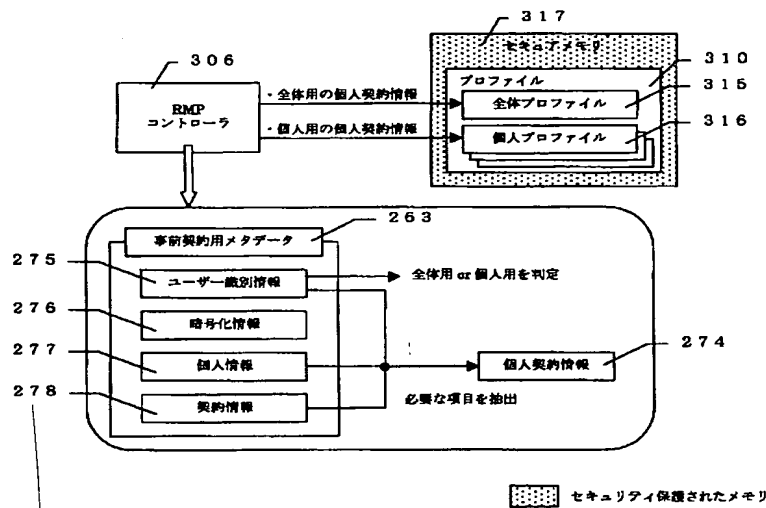
【図 42】



【図 43】



【図 44】

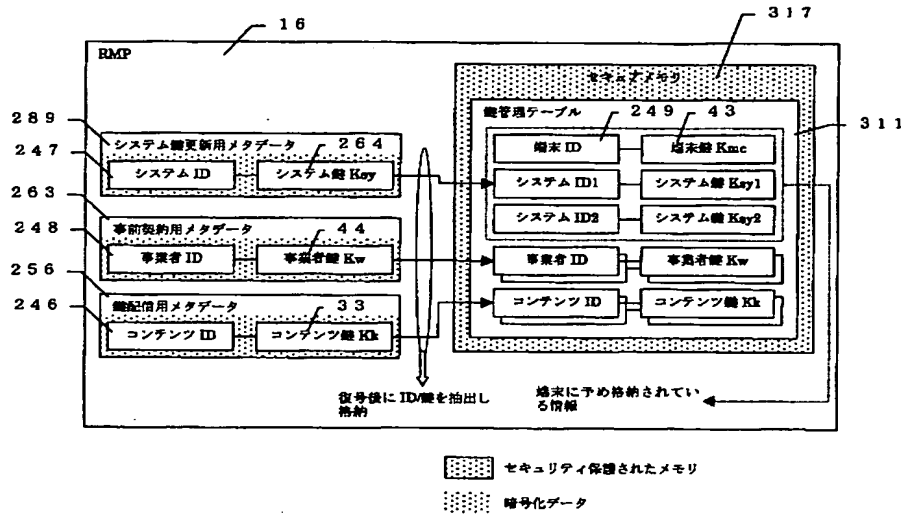


【図 51】

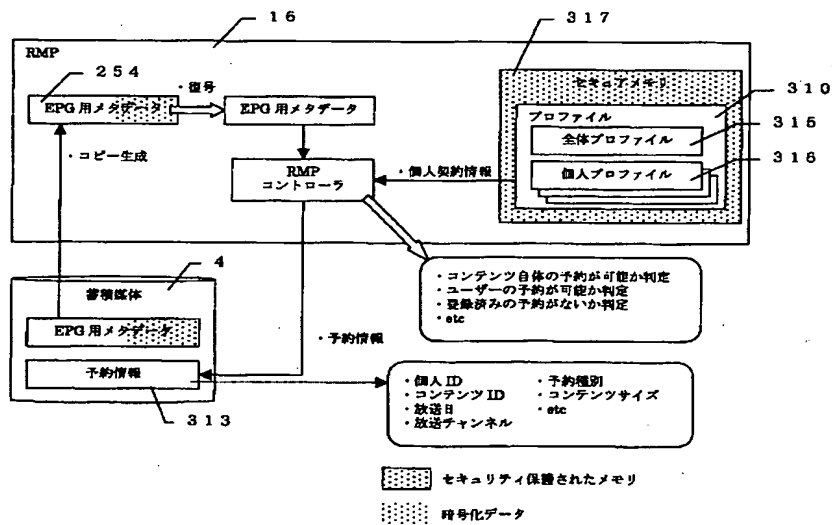
データ種別	暗号鍵種別	補足
コンテンツ	コンテンツ鍵 (Kk)	コンテンツ毎に固有の鍵
メタデータリスト	無し	暗号化を行わない
事前契約用メタデータ	端末鍵 (Kne)	端末毎に固有の鍵
EPG 用メタデータ	システム鍵 (Ksy1)	システム全体で共通の鍵
番組/再生用メタデータ	コンテンツ鍵 (Kk)	コンテンツ毎に固有の鍵
鍵配信用メタデータ (無料)	システム鍵 (Ksy1)	システム全体で共通の鍵
鍵配信用メタデータ (有料)	事業者鍵 (Kv)	事業者毎に固有の鍵
システム鍵更新用メタデータ	システム鍵 (Ksy2)	システム全体で共通の鍵 (予備用)



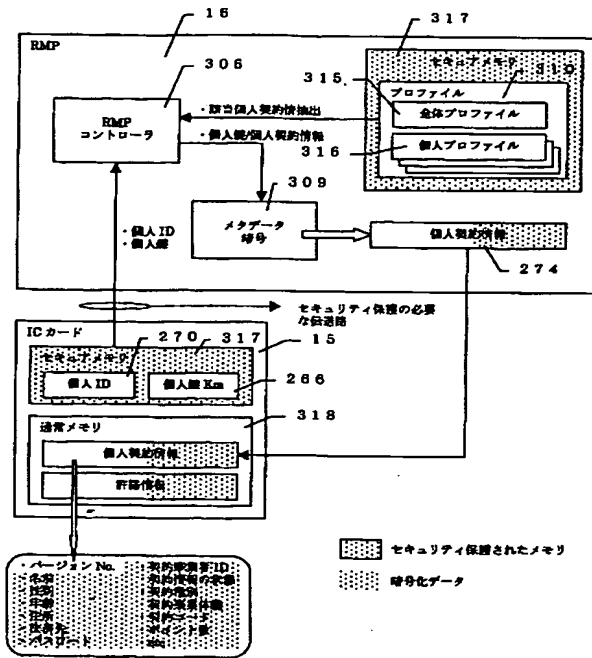
【図 45】



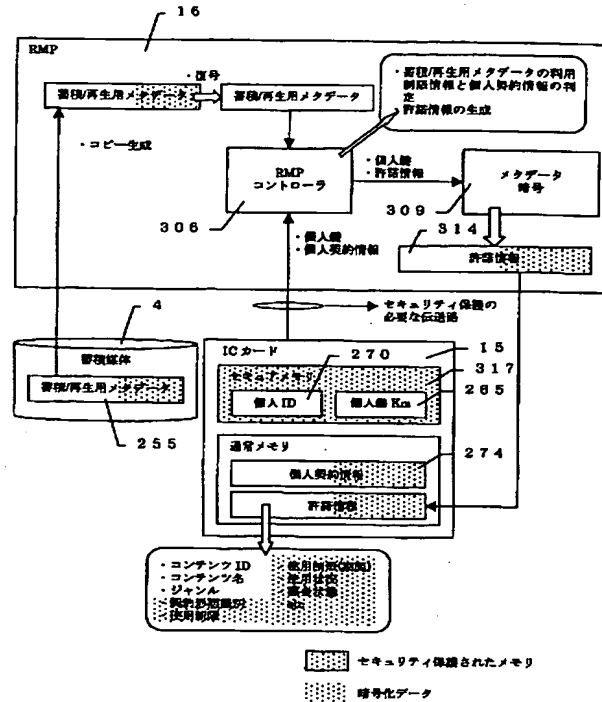
【図 47】



【図48】



【図49】



【図52】

RMP コントローラの主な機能	
機能	内容
受信制御	・著作権/再生用メタデータ、複製信用メタデータ、プロフィールより受信可能なコンテンツかを判断し、コンテンツの受信を制御する機能
著作権制御	・RMP 内部で発生するコンテンツ、メタデータ等の著作権媒体への著作権動作を EPG 用メタデータ、著作権/再生用メタデータ、メタデータリスト等により制御する機能
コピー制御	・視聴契約等のユーザーリクエスト等により発生するリムーバブルメディア等へのコピー要求を著作権/再生用メタデータの情報により制御する機能
提示制御	・ユーザーの視聴要求に対し著作権/再生用メタデータの情報、視聴契約により生成された許諾情報をもとにコンテンツの再生を制御する機能
視聴契約制御	・著作権/再生用メタデータ、IC カード内の個人契約情報をもとにコンテンツの視聴に対する許諾情報を生成する機能
課金制御	・著作権/再生用メタデータに格納されたポイント情報等と、IC カード内の個人契約情報をもとに行われる課金処理を制御する機能
個人認証制御	・各メタデータ内にユーザーを制限する情報がある場合に、プロフィール、IC カード内の個人契約情報をもとに行われる認証処理を制御する機能
鍵管理	・受信端末内の鍵を管理する機能
プロフィール管理	・事前契約用メタデータから生成される各個人、端末のプロフィールを管理する機能
時刻管理	・受信端末における時刻情報を管理する機能
アプリケーション認証制御	・Plug in アプリケーション等に対する認証を制御する機能
外部機器認証制御	・受信端末に接続される外部機器に対する認証を制御する機能
通信回線制御	・視聴履歴、課金情報等の権利保護が必要な情報を通信回線を利用し送出側に送信する際に通信路の安全性に拠る制御を行う機能

## フロントページの続き

(51)Int.Cl. <sup>7</sup>		識別記号	F I	タームコード (参考)	
H O 4 N	5/76	6 4 0	H O 4 N	7/173	6 4 0 A
	5/91		H O 4 L	9/00	6 0 1 B
	7/167		H O 4 N	7/167	Z
	7/173			5/91	P
(72)発明者 山崎 伊織 東京都千代田区神田駿河台四丁目 6 番地 株式会社日立製作所放送・通信システム推 進事業部内			Fターム(参考) 5C052 AB02 CC01 DD04 DD06 5C053 FA20 FA28 GB05 JA21 LA11 LA15 5C064 BB01 BB02 BC04 BC17 BC22 BC23 BC25 BD08 BD09 5J104 EA10 EA17 NA02 PA05 PA11		

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/007235

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> G06F17/60Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004  
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
JICST FILE (JOIS), WPI, INSPEC (DIALOG)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-279211 A (Oki Electric Industry Co., Ltd.), 27 September, 2002 (27.09.02), Figs. 1 to 2 (Family: none)	1-26
Y	JP 2002-169912 A (Hitachi, Ltd.), 14 June, 2002 (14.06.02), Full text; Figs. 1 to 13 (Family: none)	1-26
Y	JP 11-272762 A (Hitachi, Ltd.), 08 October, 1999 (08.10.99), Full text; Figs. 1 to 21 (Family: none)	1-26

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;" document member of the same patent family

Date of the actual completion of the international search  
08 July, 2004 (08.07.04)Date of mailing of the international search report  
27 July, 2004 (27.07.04)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/007235

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-83874 A (Sony Corp.), 30 March, 2001 (30.03.01), Full text & WO 1019017 A1 & JP 13-076425 A & JP 13-075871 A & JP 13-075923 A & JP 13-075930 A & JP 13-092880 A & JP 13-094554 A & EP 1128598 A & CN 1322422 A	1-26
A	JP 2000-148861 A (Sony Corp.), 30 May, 2000 (30.05.00), Full text; Figs. 1 to 15 & WO 029996 A1 & EP 1071031 A1 & CN 1293786 T & US 2001/0047317 A1 & US 2001/0047318 A1 & US 2003/0004841 A1	1-26
A	JP 2002-217894 A (Hitachi, Ltd.), 02 August, 2002 (02.08.02), Full text; Figs. 1 to 52 (Family: none)	1-26

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**